On l-adic representations of Galois groups obtained from certain two-dimensional abelian varieties

By Masami OHTA

(Communicated by Y. Ihara)

§ 0. Introduction.

Let E be an elliptic curve defined over a finite algebraic number field K, and let $\bar{K}$ be the algebraic closure of K. Then the Galois group $G=\mathrm{Gal}(\bar{K}/K)$ acts continuously on the Tate module $T_l(E)$, and we thus obtain the following l-adic representation of G for each prime number l:

$$\rho_l: \quad G \longrightarrow \mathrm{Aut}(T_l(E)) \cong GL_2(\boldsymbol{Z}_l),$$

where $\boldsymbol{Z}_l$ is the ring of l-adic integers. J.-P. Serre has proved the following

THEOREM. (Serre [3], [4]) *Assume that E does not have complex multiplication. Then*

(1) *$\rho_l(G)$ is an open subgroup of $\mathrm{Aut}(T_l(E))$ for all l.*

(2) *$\rho_l(G)=\mathrm{Aut}(T_l(E))$ for almost all l.*

In this paper, we shall prove an analogous result for certain two-dimensional abelian varieties defined over a finite algebraic number field K. Let B be an indefinite division quaternion algebra over the rational number field $\boldsymbol{Q}$, and let $\mathfrak{O}$ be a maximal order of B. Our object is a two-dimensional abelian variety A defined over K such that $\mathrm{End}(A)=\mathrm{End}_K(A)\cong\mathfrak{O}$, where $\mathrm{End}(A)$ (resp. $\mathrm{End}_K(A)$) is the ring of endomorphisms of A defined over $\bar{K}$ (resp. K).

For each prime number l, we obtain the following l-adic representation of G:

$$\rho_l: \quad G \longrightarrow \mathrm{Aut}_{\mathfrak{O}}(T_l(A)) \cong \mathfrak{O}_l^{\times},$$

where $\mathfrak{O}_l=\mathfrak{O}\otimes\boldsymbol{Z}_l$, and $\mathfrak{O}_l^{\times}$ is the unit group of $\mathfrak{O}_l$ equipped with the l-adic topology, and $\mathrm{Aut}_{\mathfrak{O}}(T_l(A))$ is the group of automorphisms of $T_l(A)$ which commute with the action of $\mathfrak{O}$ on $T_l(A)$ (for details, see Proposition 1.1). Our result is the following

THEOREM. (1) *$\rho_l(G)$ is an open subgroup of $\mathrm{Aut}_{\mathfrak{O}}(T_l(A))$ for all l.*

(2) *$\rho_l(G)=\mathrm{Aut}_{\mathfrak{O}}(T_l(A))$ for almost all l.*

The proof proceeds almost in the same way as in the Serre's papers [3], [4], [6]. Recently, I was informed that Professor J.-P. Serre had also obtained the same

result, but that it is unpublished. The present work is a part of my Master's thesis submitted to University of Tokyo, 1974 (March).

I wish to express my sincere thanks to Professor Y. Ihara whose suggestions and encouragements were invaluable.

§ 1. Preliminaries.

First we fix our notations. Let $K, B, \mathfrak{O}$, and A be as in § 0. We denote by D the discriminant of B. We put $B_l = B \otimes \boldsymbol{Q}_l$, $\mathfrak{O}_l = \mathfrak{O} \otimes \boldsymbol{Z}_l$, and denote by N_l (resp. Tr_l) the reduced norm (resp. the reduced trace) of B_l over $\boldsymbol{Q}_l$, where $\boldsymbol{Q}_l$ is the field of l-adic numbers. For a natural number n, we denote by A_n the group of n-section points of A. Then $T_l(A) = \varprojlim A_{l^n}$, and we put $V_l(A) = T_l(A) \otimes \boldsymbol{Q}_l$.

By the assumption, there is an isomorphism of $\mathfrak{O}$ onto $\mathrm{End}_K(A)$, and we identify $\mathfrak{O}$ with $\mathrm{End}_K(A)$ by this isomorphism hereafter. Especially, $\mathfrak{O}$ acts on $T_l(A)$, and B acts on $V_l(A)$.

PROPOSITION 1.1. (1) *$T_l(A)$ is isomorphic to $\mathfrak{O}_l$ as left $\mathfrak{O}$-module, and $\mathrm{Aut}_{\mathfrak{O}}(T_l(A))$ is isomorphic to $\mathfrak{O}_l^\times$, where the action of $\mathfrak{O}_l^\times$ on $T_l(A) \cong \mathfrak{O}_l$ is the right multiplication. And hence $V_l(A) \cong B_l$ as left B-module, and $\mathrm{Aut}_B(V_l(A)) \cong B_l^\times$. For each prime number l, we thus obtain an l-adic representation of G:*

$$\rho_l : \quad G \longrightarrow \mathrm{Aut}_{\mathfrak{O}}(T_l(A)) \cong \mathfrak{O}_l^\times \subset \mathrm{Aut}_B(V_l(A)) \cong B_l^\times.$$

(2) *The field generated over K by the coordinates of all the elements of A_{l^n} contains a primitive l^n-th root of unity ζ, and $\sigma \in G$ acts as $\zeta^\sigma = \zeta^{N_l(\rho_l(\sigma))}$.*

PROOF. (1) is proved in Morita [2] § 2. (2) is proved as in Shimura [9] pp. 307-309. Q.E.D.

Hereafter, we shall identify $T_l(A)$ (resp. $V_l(A)$) with $\mathfrak{O}_l$ (resp. B_l), and $\mathrm{Aut}_{\mathfrak{O}}(T_l(A))$ (resp. $\mathrm{Aut}_B(V_l(A))$) with $\mathfrak{O}_l^\times$ (resp. $B_l^\times$).

Next, we classify the l-adic Lie algebras.

PROPOSITION 1.2. *The multiplicative group $B_l^\times$ is an l-adic Lie group in the sense of Serre* [5], *and its Lie algebra $\mathfrak{B}_l$ is isomorphic over $\boldsymbol{Q}_l$ to B_l, with the bracket product $[X, Y] = XY - YX$ $(X, Y \in B_l)$. The Lie subalgebras $\mathfrak{g}$ of $\mathfrak{B}_l$ are classified as follows.*

(1) *Case $l \nmid D$.*

If $\dim \mathfrak{g}$ *(the dimension of* $\mathfrak{g}$*) is* 0 *(resp.* 4*),* $\mathfrak{g}$ *is* $\{0\}$ *(resp.* $\mathfrak{B}_l$*). If* $\dim \mathfrak{g} = 1$, $\mathfrak{g} = \{aX \mid a \in \boldsymbol{Q}_l\}$ $(X \in \mathfrak{B}_l,\ X \neq 0)$. *If* $\dim \mathfrak{g} = 2$, $\mathfrak{g}$ *is isomorphic over* $\boldsymbol{Q}_l$ *to one of the following four Lie subalgebras:* $\left\{\begin{pmatrix} a & b \\ 0 & \lambda a \end{pmatrix} \middle| a, b \in \boldsymbol{Q}_l\right\}$ $(\lambda \in \boldsymbol{Q}_l)$, $\left\{\begin{pmatrix} 0 & b \\ 0 & a \end{pmatrix} \middle| a, b \in \boldsymbol{Q}_l\right\}$,

$\left\{\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \middle| a, b \in \boldsymbol{Q}_l\right\}$, *an isomorphic image of a quadratic extension of* $\boldsymbol{Q}_l$ *into* $\mathfrak{B}_l$. (*In the third (resp. the fourth) case, we say that* $\mathfrak{g}$ *is a split (resp. non-split) Cartan subalgebra.*) *If* $\dim \mathfrak{g}=3$, $\mathfrak{g}$ *is isomorphic over* $\boldsymbol{Q}_l$ *to either* $\mathfrak{C}_l=\{X\in\mathfrak{B}_l \mid \mathrm{Tr}_l(X)=0\}$ *or* $\left\{\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \middle| a, b, c \in \boldsymbol{Q}_l\right\}$. (*In the latter case, we say that* $\mathfrak{g}$ *is a Borel subalgebra*).

(2) *Case* $l \mid D$.

If $\dim \mathfrak{g}=0$ (*resp.* 4), $\mathfrak{g}$ *is* $\{0\}$ (*resp.* $\mathfrak{B}_l$). *If* $\dim \mathfrak{g}=1$, $\mathfrak{g}=\{aX \mid a\in \boldsymbol{Q}_l\}$ $(X\in\mathfrak{B}_l$, $X\neq 0)$. *If* $\dim \mathfrak{g}=2$, $\mathfrak{g}$ *is a non-split Cartan subalgebra in the same sense as above. If* $\dim \mathfrak{g}=3$, $\mathfrak{g}=\{X\in\mathfrak{B}_l \mid \mathrm{Tr}_l(X)=0\}=\mathfrak{C}_l$.

PROOF. The first assertion is trivial. The case $l \mid D$ is well-known (cf. Serre [5] p. 7). Now assume that $l \mid D$. Then $\mathfrak{B}_l$ is the direct sum of $\boldsymbol{Q}_l$ and $\mathfrak{C}_l$, and we only have to prove that $\mathfrak{C}_l$ has no two-dimensional Lie subalgebra. But this can be checked easily by a direct computation expressing B_l in the form $B_l=\boldsymbol{Q}_l+\boldsymbol{Q}_l\cdot\alpha+\boldsymbol{Q}_l\cdot\beta+\boldsymbol{Q}_l\cdot\alpha\beta$ with $\alpha^2, \beta^2\in\boldsymbol{Q}_l$ and $\alpha\beta=-\beta\alpha$. Q.E.D.

PROPOSITION 1.3. *The Lie algebra of* $\rho_l(G)$ *cannot be* $\mathfrak{C}_l$.

PROOF. By Proposition 1.1 (2), $N_l(\rho_l(G))$ is an open subgroup of $Z_l^\times$. But the Lie subgroup of $\mathfrak{O}_l^\times$ corresponding to $\mathfrak{C}_l$ is commensurable with the subgroup $\{x\in\mathfrak{O}_l^\times \mid N_l(x)=1\}$; hence our conclusion. Q.E.D.

PROPOSITION 1.4. *A has potential good reduction at any finite prime of K.*

PROOF. This is proved in [2] § 3. It is also an easy consequence of the semi-stable reduction theorem of Grothendieck [1]. Q.E.D.

§ 2. Local results.

By Proposition 1.4, replacing K by its finite extension if necessary, we can assume that A has good reduction everywhere, and we do so hereafter.

PROPOSITION 2.1. *Let* v *be a finite prime of* K *which divides a prime number* p. *Then the* p*-rank of* $\tilde{A}=A$ *mod* v *is* 0 *or* 2. *If* p *divides* D, *it is* 0.

PROOF. The reduction mod v gives a homomorphism $V_p(A)\to V_p(\tilde{A})$. Its kernel is a B-submodule (hence a B_p-submodule) of $V_p(A)\cong B_p$. Our assertion follows at once. Q.E.D.

DEFINITION 2.2. *Let* v *be as above. We say that* A *is supersingular (resp. ordinary) at* v *if the* p*-rank of* A *mod* v *is* 0 (*resp.* 2).

Now let K_v be the completion of K at v. Put $D_v=\mathrm{Gal}(\bar{K}_v/K_v)$, and let I_v be the inertia group of v. We denote by $\mathfrak{g}, \mathfrak{d}_v, \mathfrak{i}_v$ the Lie algebras of $\rho_p(G), \rho_p(D_v), \rho_p(I_v)$

respectively.

PROPOSITION 2.3. *Let A be ordinary at v, with v dividing p. Then p does not divide D, and $\mathfrak{b}_v$ is a Borel subalgebra, and $\mathfrak{i}_v$ is isomorphic to* $\left\{\begin{pmatrix} 0 & a \\ 0 & b \end{pmatrix} \middle| a, b \in \boldsymbol{Q}_p\right\}$.

PROOF. The first assertion is already proved in Proposition 2.1. The reduction mod v gives an exact sequence of D_v-modules:

$$0 \longrightarrow X_p \longrightarrow V_p(A) \longrightarrow V_p(\tilde{A}) \longrightarrow 0,$$

with a suitable D_v-submodule X_p of $V_p(A)$. By the identification $V_p(A) \cong M_2(\boldsymbol{Q}_p)$, we can identify X_p with $\left\{\begin{pmatrix} 0 & * \\ 0 & * \end{pmatrix}\right\}$ for a suitable choice of basis, because X_p is isomorphic to an $M_2(\boldsymbol{Q}_p)$-submodule of $M_2(\boldsymbol{Q}_p)$ of dimension 2. Our conclusion follows by the same argument as that of [3] Chapter IV pp. 42-45. Q.E.D.

For the case A is supersingular, we need some lemmas.

LEMMA 2.4. *Let A be supersingular at v, and assume that $v \mid p \mid D$. Then $p \cdot 1_A = \varepsilon \cdot \pi_{p^2}$, with π_{p^2}: $\tilde{A} \to \tilde{A}^{p^2}$ the p^2-th power homomorphism, and ε: $\tilde{A}^{p^2} \to \tilde{A}$ an isomorphism.*

PROOF. This is contained in the proof of Proposition 5.3 of [9]. Q.E.D.

Now let A, v, p be as in Lemma 2.4. We denote by O_v the ring of v-integers in K_v, and by m_v the maximal ideal of O_v. Since A is supersingular at v, the D_v-module A_{p^n} is isomorphic to the D_v-module of the p^n-section points of the formal group over O_v attached to A (cf. Tate [11]). Let $f(X) = {}^t(f_1(X), f_2(X))$ be the formal power series with indeterminate $X = {}^t(X_1, X_2)$ that gives the p-times addition of this formal group. By the above lemma, $\tilde{f} = f \bmod v$ is a power series in $X^{p^2} = {}^t(X_1^{p^2}, X_2^{p^2})$, and its term of degree p^2 is of the form $\tilde{M} X^{p^2}$ with a suitable matrix $\tilde{M}$ of $GL_2(O_v/m_v)$. Let $\tilde{M}'$ be the matrix whose components are p^{-2}-th powers of those of $\tilde{M}$, and choose $M \in GL_2(O_v)$ such that $M \bmod v = \tilde{M}'$. Put $Y = MX$. Then we have

$$f(X) = f(M^{-1}Y) \equiv \begin{pmatrix} Y_1^{p^2} + (\text{terms with degree greater than } p^2) \\ Y_2^{p^2} + (\text{terms with degree greater than } p^2) \end{pmatrix} \bmod v.$$

The additive valuation v of K_v is uniquely extended to $\bar{K}_v$, and we denote it also by v. Let $\bar{O}_v$ be the ring of v-integers in $\bar{K}_v$, and $\bar{m}_v$ be the maximal ideal of $\bar{O}_v$. For $x = {}^t(x_1, x_2) \in (\bar{m}_v)^2$, we put $v(x) = \operatorname{Min}\{v(x_1), v(x_2)\}$.

LEMMA 2.5. *Put $T_n = \{x \in (\bar{m}_v)^2 \mid f^n(x) = 0\}$, where f^n is the n-th iterate of f, and put $T_n' = T_n - T_{n-1}$. Then there is a positive constant c independent of n such that the ramification index of $K_v(x) = K_v(x_1, x_2)$ over K_v is no less than cp^{2n} for all posi-*

tive integer n and any $x \in T_n'$.

PROOF. Let n_2 (resp. n_1) be the minimal integer such that $a_2 Y_2^{n_2 p^2}$ (resp. $a_1 Y_1^{n_1 p^2}$) appears in $f_1 \bmod v$ (resp. $f_2 \bmod v$) with a suitable a_2 (resp. a_1) in $(O_v/m_v)^\times$. If such n_2 (resp. n_1) does not exist, we put $n_2=\infty$ (resp. $n_1=\infty$). By the above arguments, we have

$$\begin{cases} f_1(M^{-1}Y) = A_1(Y) + Y_1^{p^2} + \varepsilon_2 Y_2^{n_2 p^2} + B_1(Y) \\ f_2(M^{-1}Y) = A_2(Y) + Y_2^{p^2} + \varepsilon_1 Y_1^{n_1 p^2} + B_2(Y), \end{cases}$$

where $A_i(Y) = 0 \bmod v$, $\varepsilon_i \in O_v^\times$ $(i=1,2)$, and each term of $B_1(Y)$ (resp. $B_2(Y)$) is divisible by either $Y_1^{p^2}$ or $Y_2^{n_2 p^2}$ (resp. $Y_2^{p^2}$ or $Y_1^{n_1 p^2}$), here the term $Y_2^{n_2 p^2}$ (resp. $Y_1^{n_1 p^2}$) is neglected if $n_2=\infty$ (resp. $n_1=\infty$). Therefore, for any $x = M^{-1}y \in (\overline{m}_v)^2$, we have

$$\begin{cases} v(f_1(M^{-1}y)) \geq \mathrm{Min}\,\{p^2 v(y_1), n_2 p^2 v(y_2), v(\xi) + v(y)\} \\ v(f_2(M^{-1}y)) \geq \mathrm{Min}\,\{p^2 v(y_2), n_1 p^2 v(y_1), v(\xi) + v(y)\}, \end{cases}$$

where ξ is a prime element of v.

Since $v(Mx) = v(x)$, and $n_i \geq 2$ $(i=1,2)$, we have

$$v(f(x)) \geq \mathrm{Min}\,\{p^2 v(x), v(\xi) + v(x)\}.$$

It is easy to see that $p^2 v(x) < v(\xi) + v(x)$ implies $v(f(x)) = p^2 v(x)$. Hence the argument in Serre [7] p. 129 is applicable. Q.E.D.

PROPOSITION 2.6. *Assume that $v \mid p \nmid D$, and that A is supersingular at v. Then* $\dim \mathfrak{i}_v \geq 2$.

PROOF. Consider the subspace $S = \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \middle| a, b \in \boldsymbol{Z}_p \right\}$ of $T_p(A) \cong M_2(\boldsymbol{Z}_p)$. If $p \nmid a$ or $p \nmid b$, the image of $t = \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}$ by the injection $S/p^n S \to T_p(A)/p^n T_p(A) \cong A_{p^n}$ is a proper p^n-section point. Fix such an element t. S is obviously an I_v-invariant subspace of $T_p(A)$, and the map of I_v to S which sends $\sigma \in I_v$ to $\sigma \cdot t \in S$ gives a morphism of p-adic analytic manifolds: $\rho_p(I_v) \to S$. Take a measure μ of S such that $\mu(S)=1$. By Lemma 2.5, $\mu(I_v \cdot t) \geq c > 0$, and hence looking at the tangent spaces, we obtain $\dim \mathfrak{i}_v \geq \dim$ (the tangent space of S at t) $=2$. Q.E.D.

PROPOSITION 2.7. *Let $v \mid p$ and A be as in Proposition* 2.6. *Then $\mathfrak{b}_v = \mathfrak{i}_v$, and it is either a non-split Cartan subalgebra or $\mathfrak{B}_p$.*

PROOF. By the above proposition and Propositions 1.2 and 1.3, we only have to prove that $\mathfrak{b}_v$ is not contained in a Borel subalgebra. Assume that $\mathfrak{b}_v$ (and hence $\mathfrak{i}_v$) is contained in a Borel subalgebra. We may assume, taking a suitable

basis of $\mathfrak{B}_p$ and replacing K by its finite extension if necessary, that $\rho_p(I_v)\subset \left\{\begin{pmatrix} * & * \\ 0 & * \end{pmatrix}\right\}\subset GL_2(\boldsymbol{Z}_p)$. Consider the subspace $S'=\left\{\begin{pmatrix} 0 & a \\ 0 & b \end{pmatrix}\middle| a, b\in \boldsymbol{Z}_p\right\}$ of $T_p(A)$. By the above assumption, $\dim (I_v\cdot t)\leq 1$ for any $t\in S'$. But, for $t=\begin{pmatrix} 0 & a \\ 0 & b \end{pmatrix}$ with $p\nmid a$ or $p\nmid b$, we have $\dim (I_v\cdot t)\geq 2$ by the same reason as in the proof of Proposition 2.6, a contradiction. The last assertion follows from the fact that I_v is a normal subgroup of D_v. Q.E.D.

THEOREM 2.8. *For all prime number p, $\rho_p(G)$ is an open subgroup of* $\mathrm{Aut}_{\mathfrak{o}}(T_p(A))$.

PROOF. First we assume that there exists a $v\mid p$ such that A is ordinary at v. Then by Proposition 2.3, the Lie algebra of $\rho_p(G)$ contains a Borel subalgebra. Assume that it is a Borel subalgebra. We may assume that $\rho_p(G)\subset\left\{\begin{pmatrix} * & * \\ 0 & * \end{pmatrix}\right\}$ by the same reason as in the proof of Proposition 2.7.

Take a finite prime v' of K. If $v'\mid p$, A cannot be supersingular at v' by Proposition 2.7. Hence by Proposition 2.3, $\mathfrak{d}_{v'}$ is also a Borel subalgebra, and $\mathfrak{d}_v$ and $\mathfrak{d}_{v'}$ are expressed as $\left\{\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}\middle| a, b, c\in \boldsymbol{Q}_p\right\}$ by a suitable coordinate system of $\mathfrak{B}_p$. And by this coordinate system, $\mathfrak{i}_v$ and $\mathfrak{i}_{v'}$ are expressed as $\left\{\begin{pmatrix} 0 & b \\ 0 & c \end{pmatrix}\middle| b, c\in \boldsymbol{Q}_p\right\}$. Hence, replacing K by its finite extension if necessary, we may assume that $I_{v'}\subset\left\{\begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix}\right\}\subset GL_2(\boldsymbol{Z}_p)$ for any $v'\mid p$.

Next, if $v'\nmid p$, we have $\rho_p(I_{v'})=\{1\}$, since A has good reduction at v'.

Hence the kernel of the map $G\to\rho_p(G)/\rho_p(G)\cap\left\{\begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix}\right\}$ corresponds to an infinite unramified abelian extension of K, a contradiction.

Next, assume that A is supersingular at any $v\mid p$, and that $\rho_p(G)$ is not open in $\mathrm{Aut}_{\mathfrak{o}}(T_p(A))$. Then, replacing K by its finite extension if necessary, we may assume that ρ_p is an abelian p-adic representation by Proposition 1.2 and Proposition 2.7. This and its restriction to D_v and I_v is semi-simple for any $v\mid p$ by Proposition 1.2 and Proposition 2.7 (cf. [7] Proposition 1). By Tate [11], ρ_p is a representation of Hodge-Tate type, and we conclude by [3] Chapter III p. 7 that ρ_p is locally algebraic (for the definition, see [3]). By the first step of this proof, all ρ_l are semi-simple (cf. [7] Proposition 1), and they form a strictly compatible system of rational l-adic representations in the sense of [3]. Therefore, by [3] Chapter III p. 15 there are infinite prime l's such that ρ_l can be brought in diagonal form. But this implies that A has complex multiplication by [3] Chapter IV p. 42. Q.E.D.

§ 3. Global results.

PROPOSITION 3.1. *Let H be a closed subgroup of $\prod_l \mathfrak{O}_l^\times$, and H_l be its projection to $\mathfrak{O}_l^\times$. For $l \nmid D$, we denote by $\tilde{H}_l$ the image of H_l by the natural map $GL_2(Z_l) \to GL_2(F_l)$. Assume:*

(1) *H_l is open in $\mathfrak{O}_l^\times$ for all l.*

(2) *The image of H by the map $\prod_l N_l$: $\prod_l \mathfrak{O}_l^\times \to \prod_l Z_l^\times$ is open.*

(3) *There exists a finite set of primes $S \supset \{l \mid l \mid D\}$ such that $\tilde{H}_l$ contains $SL_2(F_l)$ for all $l \notin S$.*

Then H is open in $\prod_l \mathfrak{O}_l^\times$.

PROOF. The argument of [3] Chapter IV pp. 23-27 is applicable. Q.E.D.

Our problem is now reduced to the study of the representation of G on A_l.

DEFINITION 3.2. *Let $v \mid p$ be a finite prime of K. We denote by $I_{v,p}$ the maximal pro-p-subgroup of I_v, and put $I_{v,t} = I_v / I_{v,p}$. For an integer d prime to p, we define a character θ_d of I_v which is trivial on $I_{v,p}$ (hence also a character of $I_{v,t}$) as follows* (cf. [4] p. 263):

$$\theta_d(\sigma) = \sigma(x^{1/d}) \cdot x^{-1/d},$$

where $\sigma \in I_v$, and x is a prime element of v in K_v. We also consider θ_d as a character with values in $\bar{F}_p^\times$ by the reduction mod v of $\bar{O}_v$.

LEMMA 3.3. (1) *For $\alpha = a/d \in \boldsymbol{Q}$ with $a, d \in \boldsymbol{Z}$, and $(a,d) = (p,d) = 1$, we put $m_\alpha = \{x \in \bar{m}_v \mid v(x) \geq \alpha\}$, $m_\alpha^+ = \{x \in \bar{m}_v \mid v(x) > \alpha\}$, and $V_\alpha = m_\alpha / m_\alpha^+$. We denote by $\tilde{\sigma}$ the image of $\sigma \in D_v$ by the natural map $D_v \to \mathrm{Gal}(\bar{k}_v / k_v)$, where k_v is the residue field of v. Then V_α is a one-dimensional vector space over $\bar{k}_v$, and $\sigma \in D_v$ acts on V_α $\tilde{\sigma}$-linearly. In particular, I_v acts on V_α linearly, and its action is given by the character θ_d^a.*

(2) *Let μ_p be the group of p-th roots of unity in $\bar{K}_v$, and let e be the ramification index of K_v over $\boldsymbol{Q}_p$. Then the action of I_v on μ_p is given by the character θ_{p-1}^e.*

PROOF. This is Propositions 6, 7, 8 of [4]. Q.E.D.

Hereafter, we consider only those primes p which are unramified in K and $p \nmid D$. We then obtain a representation for each such p:

$$\varphi_p: \quad D_v \longrightarrow \mathrm{Aut}_{\mathfrak{O}}(T_p(A)/pT_p(A)) \cong GL_2(F_p).$$

PROPOSITION 3.4. *Take a prime $v \mid p$, and assume that A is ordinary at v. Consider the representation*

$$\varphi_p: \quad I_v \longrightarrow \mathrm{Aut}_{\mathfrak{O}}(T_p(A)/pT_p(A)) \cong GL_2(F_p).$$

Then

(1) *φ_p is equivalent to the representation* $\begin{pmatrix} 1 & * \\ 0 & \theta_{p-1} \end{pmatrix}$ *with suitable* $*$.

(2) *If $I_{v,p}$ acts on A_p non-trivially, the order of $\varphi_p(I_v)$ is $p(p-1)$.*

(3) *If $I_{v,p}$ acts on A_p trivially, the order of $\varphi_p(I_v)$ is $p-1$.*

PROOF. By the reduction mod v, we obtain the exact sequence of D_v-modules:

$$0 \longrightarrow X_p \longrightarrow A_p \longrightarrow (A \bmod v)_p \longrightarrow 0.$$

We can identify A_p with $M_2(\boldsymbol{F}_p)$, and X_p with $\left\{\begin{pmatrix} 0 & * \\ 0 & * \end{pmatrix}\right\}$. Our conclusion follows from Proposition 1.1 (2) and Lemma 3.3 (2), using the same argument as [4] pp. 273-274. Q.E.D.

LEMMA 3.5. *Take a prime v of K such that $v|p \nmid D$, and assume that A is supersingular at v. If we normalize v by $v(p)=1$, we have $v(x)=1/(p^2-1)$ for all $x \in T_1'$, where T_1' is as in Lemma 2.5.*

PROOF. Since we are assuming that p is unramified in K, we can take p as a prime element of K_v. Let $f(X)={}^t(f_1(X), f_2(X))$, M, etc. be as in §2, and put $y=Mx$. We may assume that $v(y_2) \leq v(y_1)$, i.e. $v(y_2)=v(y)$ by symmetry. First we see that

$$f_2(M^{-1}Y)\,Y_2^{-1} \equiv Y_2^{p^2-1} + \varepsilon_1 Y_1^{n_1 p^2} Y_2^{-1} + B_2(Y)\,Y_2^{-1} \bmod v.$$

If $v(y)=v(y_2)<1/(p^2-1)$, we have

$$1 > v(y_2^{p^2-1}) \geq \operatorname{Min}\{1=v(p), v(y_1^{n_1 p^2} \cdot y_2^{-1})\}.$$

Hence we have $n_1<\infty$, and $(p^2-1)v(y_2) \geq n_1 p^2 v(y_1) - v(y_2) > (p^2-1)v(y_2)$, a contradiction. Therefore, we have $v(y_2) \geq 1/(p^2-1)$.

Next, put $M^{-1}=\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$. Since $f(X)=pX+$(terms with degree greater than 1), we have

$$f(M^{-1}Y)=\begin{pmatrix} p(\alpha Y_1+\beta Y_2)+pC_1(Y)+Y_1^{p^2}+\varepsilon_2 Y_2^{n_2 p^2}+B_1(Y) \\ p(\gamma Y_2+\delta Y_2)+pC_2(Y)+Y_2^{p^2}+\varepsilon_1 Y_1^{n_1 p^2}+B_2(Y) \end{pmatrix}$$

where each term of $C_i(Y)$ has degree greater than 1, and $B_i(Y)$ is as in the proof of Lemma 2.5.

Since $v(M^{-1}y)=v(y)$, we have either $v(\alpha y_1+\beta y_2)=v(y_2)$, or $v(\gamma y_1+\delta y_2)=v(y_2)$. Assume that $v(\alpha y_1+\beta y_2)=v(y_2)$. Then $f(M^{-1}y)=0$ implies

$$1+v(y_2)=v(p(\alpha y_1+\beta y_2))=v(pC_1(y)+y_1^{p^2}+\varepsilon_2 y_2^{n_2 p^2}+B_1(y)).$$

But by the above argument, we have

$$v(y_2^{n_2 p^{2p^2}}) = n_2 p^2 v(y_2) > (p^2-1)v(y_2) + v(y_2) \geq 1 + v(y_2),$$

if $n_2 < \infty$. Therefore $1 + v(y_2) \geq p^2 v(y_1) \geq p^2 v(y_2)$, and hence $v(y_2) \leq 1/(p^2-1)$.

The proof in the case $v(\gamma y_1 + \delta y_2) = v(y_2)$ is similar. Q.E.D.

PROPOSITION 3.6. *Let $v|p$, and A be as in Lemma 3.5. Then A_p is isomorphic to a two-dimensional vector space over $\boldsymbol{F}_{p^2}$, and the action of $\sigma \in I_v$ is a multiplication of $\theta_{p^2-1}(\sigma)$ on this vector space. The image of D_v by φ_p is either a cyclic group of order p^2-1, or its normalizer in $GL_2(\boldsymbol{F}_p)$. The former case occurs if and only if the residue field of v contains $\boldsymbol{F}_{p^2}$.*

PROOF. By Lemma 3.5, we have an injective map of D_v-modules: $T_1 \to V_\alpha \oplus V_\alpha$ with $\alpha = 1/(p^2-1)$ by sending $x = {}^t(x_1, x_2) \in T_1$ to $(x_1 \bmod m_\alpha^+,\ x_2 \bmod m_\alpha^+) \in V_\alpha \oplus V_\alpha$. Our assertion follows from Lemma 3.3 (1). Q.E.D.

THEOREM 3.7. *There exists a finite set of primes $S \supset \{l | l | D$, or $l \leq 7$, or l is ramified in $K\}$ such that $\varphi_l(G) = GL_2(\boldsymbol{F}_l)$ for all $l \notin S$.*

PROOF. After Proposition 3.4 and Proposition 3.6, we can proceed thoroughly in the same way as in [4] §4, and we omit the proof although it is the essential part of the proof. Q.E.D.

We have now established the theorem of §0 by Proposition 3.1.

Finally, let us consider the case $\mathrm{End}_K(A) = \mathrm{End}(A) \cong \mathfrak{x}$, where K and A are as before, but $\mathfrak{x}$ is an order of B which may not be maximal. Take a maximal order $\mathfrak{O}$ which contains $\mathfrak{x}$, and put $\mathfrak{k} = \{x \in B | x\mathfrak{O} \subseteq \mathfrak{x}\}$. One sees easily that $\mathfrak{k}$ is a lattice in B contained in $\mathfrak{x}$, and that the right order of $\mathfrak{k}$ is $\mathfrak{O}$. Therefore by Shimura-Taniyama [10] §7 Proposition 7, there is a $\mathfrak{k}$-transform A' of A defined over K, which has the property $\mathrm{End}_K(A') = \mathrm{End}(A') \cong \mathfrak{O}$. Moreover, we can take a $\mathfrak{k}$-multiplication of A onto A' defined over K by loc. cit. Hence $V_l(A)$ and $V_l(A')$ are isomorphic as G-modules, and the l-adic representation of G on $V_l(A)$ is equivalent to that on $V_l(A')$ for each prime number l.

References

[1] Grothendieck, A., (avec la collaboration de M. Raynaud et D. S. Rim), Groupes de Monodromie en Géométrie Algébrique (S.G.A. 7I), Springer lecture note 288.

[2] Morita, Y., Ihara's conjectures and moduli spaces of abelian varieties, to appear in J. Math. Soc. Japan.

[3] Serre, J.-P., Abelian l-adic Representations and Elliptic Curves, Benjamin, 1968.

[4] Serre, J.-P., Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, Invent. Math. **15** (1972), 259-331.

[5] Serre, J.-P., Sur les groupes de congruence des variétés abéliennes, Izv. Akad. Nauk. S.S.S.R. **28** (1964), 3-20.
[6] Serre, J.-P., Groupes de Lie l-adiques attachés aux courbes elliptiques, Colloq. Clermont-Ferrand, C.N.R.S., 1964, 239-256.
[7] Serre, J.-P., Sur les groupes de Galois attachés aux groupes p-divisibles, Proc. Conf. on Local Fields, Springer, 1967, 113-131.
[8] Serre, J.-P., Lie Algebras and Lie Groups, Benjamin, 1965.
[9] Shimura, G., On the zeta functions of the algebraic curves uniformized by certain automorphic functions, J. Math. Soc. Japan. **13** (1961), 275-331.
[10] Shimura, G., and Y. Taniyama, Complex multiplication of abelian varieties and its applications to number theory, Publ. Math. Soc. Japan, No. 6, 1961.
[11] Tate, J., p-divisible groups, Proc. Conf. on Local Fields, Springer, 1967, 158-183.

(Received March 7, 1974)

Department of Mathematics
Kyoto University
Kyoto
606 Japan