T. NAKAMURA
KŌDAI MATH. SEM. REP
28 (1976), 110—114

ON l-ADIC REPRESENTATIONS ATTACHED TO CERTAIN ABELIAN VARIETIES OVER ALGEBRAIC NUMBER FIELDS

BY TETSUO NAKAMURA

Let K be a field and let A be an abelian variety defined over K, of dimension g. Let l be a prime number different from the characteristic of K and let $T_l(A)$ be the Tate module of A. Let $V_l(A)=T_l(A)\otimes_{\mathbf{Z}_l}\mathbf{Q}_l$. The Galois group $G_K=\mathrm{Gal}(K_s/K)$ operates both on $T_l(A)$ and $V_l(A)$. Write $\mathrm{End}(A)$ and $\mathrm{End}_K(A)$ for the rings of all endomorphisms of A and of K-endomorphisms of A, respectively. Then it is well known that the canonical map

$$\mathbf{Q}_l\otimes\mathrm{End}_K(A)\longrightarrow\mathrm{End}_{G_K}(V_l(A)) \tag{1}$$

is injective. It is conjectured that the map (1) is bijective for a field K which is finitely generated over the prime field. Tate [8] has proved this in case K is a finite field.

Let K be an algebraic number field. Let v be a place of K. We denote by K_v the completion of K with respect to v and by k_v its residue field. Let l be a prime number different from the characteristic p_v of k_v. If A has good reduction at v, we have the following canonical commuting diagram of injective homomorphisms

$$\begin{array}{ccc}\mathbf{Q}_l\otimes\mathrm{End}_K(A) & \longrightarrow & \mathrm{End}\,(V_l(A))\\ \downarrow & & \wr\downarrow\\ \mathbf{Q}_l\otimes\mathrm{End}_{k_v}(\tilde{A}_v) & \longrightarrow & \mathrm{End}\,(V_l(\tilde{A}_v)),\end{array}$$

where $\tilde{A}_v$ is the reduction of A at v. Since the Galois module $V_l(A)$ is unramified at v, the natural operations of G_K and G_{k_v} are compatible in the diagram. In this paper we shall consider that $\mathrm{End}_K(A)\otimes\mathbf{Q}_l$ is embedded in $\mathrm{End}\,(V_l(A))$ and identify $\mathrm{End}\,(V_l(A))$ with $M_{2g}(\mathbf{Q}_l)$, the total matrix ring of degree $2g$ over $\mathbf{Q}_l$.

Now consider an abelian variety A defined over an algebraic number field K, satisfying the following two properties:

(P1) $E=\mathrm{End}\,(A)\otimes\mathbf{Q}=\mathrm{End}_K(A)\otimes\mathbf{Q}$ is a totally real field of degree g over $\mathbf{Q}$.

(P2) There exist two places v_1 and v_2 of K where A has good reduction such that $E_i=\mathrm{End}_{k_{v_i}}(\tilde{A}_{v_i})\otimes\mathbf{Q}=\mathrm{End}(\tilde{A}_{v_i})\otimes\mathbf{Q}$ $(i=1, 2)$ are fields of degree $2g$ over

Received Oct. 1, 1975.

$\mathbf{Q}$ and such that they are not isomorphic over E.

For such an abelian variety A we shall prove the following; for every prime number l, $V_l(A)$ is a semi-simple G_K-module and the map (1) is bijective. Applying the above result, it is possible to determine the l-adic Lie algebra of $\rho_l(G_K)$, where ρ_l is a l-adic representation attached to A. For an abelian variety A which satisfies (P1), Ribet [4] has obtained the similar results assuming, instead of (P2), that A does not have everywhere potential good reduction.

It should be noted that the condition (P2) is not so much extraordinary for simple abelian varieties which satisfy (P1). The jacobian varieties of the elliptic modular function fields corresponding to the groups $\Gamma_0(23)$, $\Gamma_0(29)$, $\Gamma_0(31)$, (They are all of dimension 2.) and $\Gamma_0(41)$ (of dimension 3) satisfy (P1) and (P2). (cf. Doi [2]. Matsui [3]) Also abelian varieties in Casselman [1], which will be treated in the last of the paper, satisfy these properties.

1. Let K be an algebraic number field and let A be an abelian variety of dimension g defined over K such that (P1) and (P2) are satisfied. Let l be a prime number. Let $E_l=E\otimes\mathbf{Q}_l=\prod_{\lambda|l}E_\lambda$, where λ ranges over all places of E lying above l and E_λ is the completion of E at λ. Since $V_l(A)$ is a free module of rank 2 over $E_l=\mathrm{End}(A)\otimes\mathbf{Q}_l$, $V_l(A)$ is canonically decomposed as $\prod_{\lambda|l}V_\lambda$, where each V_λ is a E_λ-space of dimension 2. As V_λ is a G_K-module, it defines λ-adic representation $\rho_\lambda: G_K\to\mathrm{Aut}(V_\lambda)$. (ρ_λ), where λ runs over all places of E, forms a compatible system of E-rational λ-adic representations of degree 2. (For details of the above facts, see Shimura [6], §7.6, Serre [5], I-13 and Ribet [4], Chap. I, II.) It is a result of Tate [9] and Raynaud (unpublished) that $V_l(A)$ is a Hodge-Tate module. (For Hodge-Tate modules and representations, see Serre, l. c., Chap. III.)

LEMMA 1. *Let λ be a place of E and ρ_λ be as above. If the semi-simplification $\hat{\rho}_\lambda$ of ρ_λ is abelian, then $\hat{\rho}_\lambda$ is a locally algebraic representation in the sense of Serre, l. c..*

Proof. Regarding V_λ as a vector space over $\mathbf{Q}_l$, we denote it by W. Then from the natural injection $\alpha: \mathrm{Aut}(V_\lambda)\to\mathrm{Aut}(W)$, we obtain an algebraic morphism $\bar{\alpha}: GL_{V_\lambda}\to GL_W$, which is defined over E_λ. Let $\eta: G_K\to\mathrm{Aut}(W)$ be defined by $\eta=\alpha\circ\hat{\rho}_\lambda$. Then η is a semi-simple abelian l-adic representation. Since submodules and quotient modules of a Hodge-Tate module are also Hodge-Tate modules, η is locally algebraic. (cf. Serre, l. c.) Therefore there exists an algebraic morphism $r: T\to GL_W$, defined over $\mathbf{Q}_l$, such that $r(x^{-1})=\eta\circ i_l(x)$ for $x\in K_l^\times=(K\otimes\mathbf{Q}_l)^\times$ close enough to 1, where T is a $\mathbf{Q}_l$-torus such that $T(\mathbf{Q}_l)=(K\otimes\mathbf{Q}_l)^\times$ and where $i_l: K_l^\times\to G_K{}^{ab}$ is the canonical homomorphism of class field theory. By definition of η, the image of some open neighborhood of 1 in $K_l^\times$ by $\eta\circ i_l$, which is Zariski dense in $\mathrm{Im}(r)$, is contained in the image of α. This shows that there exists a morphism $f: T\to GL_{V_\lambda}$, defined over E_λ, such that $r=\bar{\alpha}\circ f$. Hence we have that $f(x^{-1})=\hat{\rho}_\lambda\circ i_l(x)$ for $x\in K_l^\times$ close enough to 1. Thus our lemma is proved.

COROLLARY. *If there exists a place λ_0 of E such that $\hat{\rho}_{\lambda_0}$ is abelian, then for every place λ, $\hat{\rho}_\lambda$ is abelian.*

Proof. By Lemma 1, $\hat{\rho}_{\lambda_0}$ is a locally algebraic abelian semi-simple representation. Since $(\hat{\rho}_\lambda)$ forms a compatible system of semi-simple λ-adic representations, they come from an E-linear representation of some S_m. (cf. Serre [5], III-16) Therefore, for every λ, $\hat{\rho}_\lambda$ is abelian.

Now let F_λ be the $\mathbf{Q}_l$-subalgebra generated by $\rho_\lambda(G_K)$ in $\mathrm{End}(V_\lambda)$, and let $F_l=\prod_{\lambda | l} F_\lambda$. (direct sum in $\mathrm{End}(V_l(A))$ Then F_l is the $\mathbf{Q}_l$-subalgebra generated by $\rho_l(G_K)$ in $\mathrm{End}(V_l(A))$.

LEMMA 2. *Let F_λ be as above. Then $F_\lambda \supset E_\lambda$.*

Proof. For a place v of K where A has good reduction, let σ_v be a Frobenius element in G_K with respect to v. If $l\neq p_v$, $\rho_l(\sigma_v)$ corresponds to the Frobenius endomorphism f_v of $\tilde{A}_v$ relative to k_v. Denote by a_v the trace of $\rho_\lambda(\sigma_v)$ for $\lambda | l$. Then $a_v \in E$ and it is independent of the choice of l $(\neq p_v)$ and λ. Let Φ be the field over $\mathbf{Q}$ generated by all a_v. Then $\Phi\subset E$. Let S be any finite set of places of K which contains all places of K where A has bad reduction. Then Čebotarev's density theorem shows that $\Phi=\mathbf{Q}(\{a_v\}_{v\notin S})$. Now by (P2) we have $\mathbf{Q}(f_{v_i}+\bar{f}_{v_i})=E$ $(i=1, 2)$, hence $\Phi=E$. Therefore we have $F_\lambda\supset E_\lambda$.

PROPOSITION 1. *$\hat{\rho}_\lambda$ is not abelian for each place λ of E.*

Proof. Let l $(\neq p_{v_1}, p_{v_2})$ be a prime number such that $E_1\otimes\mathbf{Q}_l$ and $E_2\otimes\mathbf{Q}_l$ are not isomorphic as $E\otimes\mathbf{Q}_l$-algebras. The existence of such a l is obvious because of (P2) and Čebotarev's density theorem. In view of the corollary of Lemma 1, it suffices to show that $\hat{\rho}_l$ is not abelian, since $\hat{\rho}_l$ is the direct sum of $\hat{\rho}_\lambda$ (considered as l-adic representation). Now suppose $\hat{\rho}_l$ is abelian. Since $F_l\supset E_i\otimes\mathbf{Q}_l$ $(i=1, 2)$ by (P2), we have that the semi-simplification $\hat{F}_l$ of F_l contains $E_i\otimes\mathbf{Q}_l$. Therefore we have $\hat{F}_l=E_1\otimes\mathbf{Q}_l=E_2\otimes\mathbf{Q}_l$. However the choice of l gives a contradiction and hence $\hat{\rho}_l$ is not abelian. This completes the proof.

THEOREM 1. *For every rational prime l, $V_l(A)$ is a semi-simple G_K-module and the map* (1) *is bijective.*

Proof. By Proposition 1, we can easily deduce that V_λ is a simple $E_\lambda[G_K]$-module and, therefore, V_λ is a semi-simple $\mathbf{Q}_l[G_K]$-module; so $V_l(A)$ is semi-simple. Hence to complete the proof it suffices to show that the commutor of F_l is E_l and hence that the commutor of F_λ in $\mathrm{End}_{\mathbf{Q}_l}(V_\lambda)$ (=all endomorphisms of V_λ considered as $\mathbf{Q}_l$-space) is E_λ, which is clear by Lemma 2 and Proposition 1.

Remark. The assertion of Theorem 1 remains true even if K is replaced by a finite extension of K, since (P1) and (P2) are unchanged.

THEOREM 2. *For each prime number l, let $\mathfrak{g}_l$ be the l-adic Lie algebra of $\rho_l(G_K)$ in $M_{2g}(\mathbf{Q}_l)$. Then*

$$\mathfrak{g}_l \cong \mathbf{Q}_l \cdot I \oplus (\bigoplus_{\lambda | l} \mathfrak{sl}_2(E_\lambda)),$$

where I is the unit matrix and where $\mathfrak{sl}_2(E_\lambda)=\left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(E_\lambda) \mid a+d=0\right\}$ and $\mathfrak{sl}_2(E_\lambda)$ are diagonally embedded in $M_{2g}(\mathbf{Q}_l)$ in the obvious manner. (Theorem 2 follows from Theorem 1 directly, but we omit its proof since it is essentially contained in Ribet [4], Chap. IV.)

Remark. Let G_l be the canonical image of $\rho_l(G_K)$ in $\mathrm{Aut}(T_l(A)/lT_l(A))$. Then Ribet [4], Chap. V, determined G_l for almost all l if A satisfies (P1) and does not have everywhere potential good reduction. It is still true if A satisfies (P1) and (P2). The proof in Ribet, l. c., is clearly applicable to our case by the preceding considerations.

2. Let N be a prime such that $N \equiv 1$ (mod. 4); let $k=\mathbf{Q}(\sqrt{N})$ and let $\psi(a) = \left(\frac{N}{a}\right)$ be the Legendre symbol. Then there exist an abelian variety A defined over $\mathbf{Q}$ and an abelian subvariety A' defined over k such that $A'+A'^{\varepsilon}=A$ and A is isogenous to $A' \times A'$ over k, where ε is the generator of $\mathrm{Gal}(k/\mathbf{Q})$. Further there exists a CM field K of degree $\dim(A)$ with an embedding $\theta: K \to \mathrm{End}(A) \otimes \mathbf{Q}$. Let K' be the maximal real subfield of K. Then we can define an embedding θ' of K' into $\mathrm{End}(A') \otimes \mathbf{Q}$ so that $\theta'(s)$ is the restriction of $\theta(s)$ to A' for every $s \in K'$. Let p $(\neq N)$ be a prime and $\mathfrak{p}$ be a prime ideal of k dividing p. Let the tilde denote reduction mod $\mathfrak{p}$. Let π_p be the Frobenius endomorphism of $\tilde{A}$ of degree p and π_p^* be the element of $\mathrm{End}(\tilde{A})$ such that $\pi_p \cdot \pi_p^* = p$. Then we have $\pi_p + \psi(p) \cdot \pi_p^* = \tilde{\theta}(a_p)$, where a_p is the eigen value of the Hecke operator acting on the cusp form associated to A. (For these abelian varieties, see Shimura [6], Chap. 7, and Casselman [1].) If $N=29$, 53, 61, 73, 89, or 97, A' is simple and not of CM type (so A' satisfies (P1).) and Casselman (l. c.) proved that A' has good reduction at each place of k. Now let $N=73$. Then $K' = \mathbf{Q}(\sqrt{5})$ and $\dim A'=2$. We show that in this case A' satisfies (P2). For $p=2$ and 3, a_p satisfy the equations $X^2+X-1=0$ and $X^2-X-1=0$, respectively. (cf. Wada [9]) Since $\psi(2)=\psi(3)=1$, we can compute π_2 and π_3. Then $\mathbf{Q}(\pi_2)/\mathbf{Q}$ and $\mathbf{Q}(\pi_3)/\mathbf{Q}$ are not Galois extensions and the prime ideal (41) is ramified in $\mathbf{Q}(\pi_2)/\mathbf{Q}$ and unramified in $\mathbf{Q}(\pi_3)/\mathbf{Q}$. These facts show that A' satisfies (P2).

If $N=97$, then $\dim(A')=3$ and a_p satisfy the equation $X^3-3X-1=0$ for $p=2$ and $p=3$. (cf. [9]) In this case we also easily see that A' satisfies (P1) and (P2).

REFERENCES

[1] W. CASSELMAN, On abelian varieties with many endomorphisms and a conjecture of Shimura's Inventiones Math., 12, 225-236 (1971).

[2] K. DOI, On the jacobian varieties of the fields of elliptic modular functions. Osaka Math. J., 15, 249-256 (1963).

[3] T. MATSUI, On the endomorphism algebra of jacobian varieties attached to the fields of elliptic modular functions. Osaka J. Math., 1, 25-31 (1964).

[4] K. A. RIBET, Galois action on division points of abelian varieties with many real multiplications. Thesis, Harvard Univ. (1973).

[5] J.-P. SERRE, Abelian l-adic representations and elliptic curves. New York: Benjamin (1968).

[6] G. SHIMURA, Introduction to the arithmetic theory of automorphic functions. Publ. Math. Soc. Japan, No. 11, Iwanami Shoten and Princeton Univ. Press (1971).

[7] J. TATE, p-divisible groups. Proc. Conf. on Local Fields, Springer, 158-183 (1967).

[8] J. TATE, Endomorphisms of abelian varieties over finite fields. Inventiones Math., 2, 134-144 (1966).

[9] H. WADA, Tables of Hecke operators (I). United States-Japan Seminar on Modern Methods in Number Theory, Tokyo Univ., 1-10 (1971).

DEPARTMENT OF MATHEMATICS,
COLLEGE OF GENERAL EDUCATION
TOHOKU UUNIVERSITY.