Matsui, T.
Osaka J. Math.
1 (1964), 25-31

ON THE ENDOMORPHISM ALGEBRA OF JACOBIAN VARIETIES ATTACHED TO THE FIELDS OF ELLIPTIC MODULAR FUNCTIONS

TOKUJI MATSUI

(Received December 19, 1963)

In this paper we study in detail some of fields of elliptic modular functions and their jacobian varieties. In this direction we have a recent work of K. Doi [1] who answered partially to the problem proposed by E. Hecke, Y. Taniyama and G. Shimura to study the properties of jacobian varieities of elliptic modular function fields. He showed in particular, the existence of jacobian varieties of this kind which do not admit decomposition into a product of elliptic curves (in the sense of isogeny). He obtained this result by showing that there are jacobian varieties of this kind for which the rings of endomorphisms are isomorphic to real quadratic number fields (as is well known, an abelian variety is simple if and only if the ring of endomorphisms is a division algebra). His examples concern to the elliptic modular function fields corresponding to the group $\Gamma_0(N)$ with $N=22$, 23, 29, 31 and 37, where the genus of the fields (*i.e.* the dimension of corresponding jacobian varieties) is 2.

In the present note we carry out calculations similar to his in more complicated cases of higher genus (by employing slightly improved technics). The result obtained is as follows; The jacobian varieties $J_{\Gamma_0(41)}$ and $J_{\Gamma_0(47)}$ corresponding to elliptic modular groups $\Gamma_0(N)$ with $N=41$ and 47, are both *simple* abelian varieties of dimension 3 and 4, respectively. In the first case, the ring of endomorphisms is isomorphic to a totally real algebraic number field of degree 4 (of which we later give a full description). In the latter case we calculate the ring of endomorphisms of the reduction $\tilde{J}_{\Gamma_0(47)}$ of $J_{\Gamma_0(47)}$ mod 5, instead of that of $J_{\Gamma_0(47)}$ itself, which turns out to be isomorphic to an algebraic number field of degree 8. This sole fact is enough for the simplicity of $J_{\Gamma_0(47)}$ since an abelian variety is simple whenever a reduction (modulo some prime number) is simple.

1. Criterion for $J_{\Gamma_0(N)}$ to be simple. In this section, we shall prove a criterion for the jacobian variety $J_{\Gamma_0(N)}$ to be simple, in slightly improved form than [1] for the group $\Gamma_0(N)$ of genus g.

1.1. Let $\tau_{p,1}, \cdots, \tau_{p,g}$ be the eigenvalues of the Hecke operator T_p acting on the space of cusp-forms of degree-2, and let $\pi_{p,j}$ $(j=1, \cdots, 2g)$ be the eigenvalues of an l-adic representation $M_l(\pi_p)$ of p-th power endomorphism π_p of $\tilde{J}_{\Gamma_0}(N)$ (reduction of $J_{\Gamma_0(N)} \bmod p$). Then, denoting with $\bar{\pi}_{p,j}$ $(=\pi_{p,j'})$ the complex conjugate of $\pi_{p,j}$, $\pi_{p,j}$ and $\bar{\pi}_{p,j}$ satisfy an equation

$$X^2-\tau_{p,i}X+p = 0$$

for some $\tau_{p,i}$ $(1\leqq i\leqq g)$ (cf. the proof of Lemma 2 of [1]). We assume, without loss of generality, $\pi_{p,1}$ and $\bar{\pi}_{p,1}$ satisfy

$$X^2-\tau_{p,1}X+p = 0$$

we remark that if the characteristic polynomial of $M_l(\pi_p)$ is irreducible over $\boldsymbol{Q}$, we can identify $\pi_{p,1}$ with an element of the endomorphism ring $\mathcal{A}_0(\tilde{J}_{\Gamma_0(N)})$ of $\tilde{J}_{\Gamma_0(N)}$ and set $\boldsymbol{Q}(\pi_{p,1})\subset\mathcal{A}_0(\tilde{J}_{\Gamma_0(N)})$. Now we have in [1] the following criterion due to G. Shimura:

Criterion (A). Let $J_{\Gamma_0(N)}$ be the jacobian variety of dimension g corresponding to $\Gamma_0(N)$, g being the genus of $\Gamma_0(N)$. Let $\tilde{J}_{\Gamma_0(N)}$ denote the reduction of $J_{\Gamma_0(N)} \bmod p$, where p is a prime number not dividing $6N$. Assume that

P1) $[\boldsymbol{Q}(\tau_{p,1}):\boldsymbol{Q}] = g$

P2) $[\boldsymbol{Q}(\pi_{p,1}^m):\boldsymbol{Q}] = 2g$ for every positive

integer m,
then $\mathcal{A}_0(\tilde{J}_{\Gamma_0(N)})$ is isomorphic to $\boldsymbol{Q}(\pi_{p,1})$ and $\tilde{J}_{\Gamma_0(N)}$ and hence $J_{\Gamma_0(N)}$ are simple abelian varieties.

1.2. Now we proceed to replace P2) by other conditions convenient to apply to the case of $\Gamma_0(N)$ of higher genus.

Proposition 1. *Let notations be the same as above and suppose that the following conditions are satisfied*;

P1) $[\boldsymbol{Q}(\tau_{p,1}):\boldsymbol{Q}] = g$

P2)′ $[\boldsymbol{Q}(\pi_{p,1}):\boldsymbol{Q}] = 2g$

Q1) $\boldsymbol{Q}(\tau_{p,1})$ *is the unique maximal subfield of* $\boldsymbol{Q}(\pi_{p,1})$.

Then, the condition P2) *in the criterion above is equivalent to*

Q2) $\pi_{p,1}^m$ *is not contained in* $\boldsymbol{Q}(\tau_{p,1})$ *for any positive integer* m.

Proof. P2)$\Rightarrow$Q2) is obvious.

Conversely, if $\boldsymbol{Q}(\pi_{p,1}^m) \subsetneqq \boldsymbol{Q}(\pi_{p,1})$ for some positive integer m, then by Q1), $\boldsymbol{Q}(\pi_{p,1}^m) \subseteqq \boldsymbol{Q}(\tau_{p,1})$. This contradicts to the condition Q2).

Criterion (B). Let $J_{\Gamma_0(N)}$, $\tilde{J}_{\Gamma_0(N)}$ and p be of the same meaning as in criterion (A). The conclusions of criterion (A) hold if the conditions P1), P2)′, Q1), and the following Q2)′ are satisfied;
Q2)′ $(\tau_{p,1}, p)=1$ (or equivalently, $(N_{\boldsymbol{Q}(\tau_{p,1})/\boldsymbol{Q}}(\tau_{p,1}), p)=1$).

Proof. By proposition 1 above, we have only to prove that the conditions Q1) and Q2)′ imply Q2). Suppose the contrary of Q2), ie $\pi_{p,1}^m \in \boldsymbol{Q}(\tau_{p,1})$ for some integer m. Then $\pi_{p,1}^m = \bar{\pi}_{p,1}^m$, and hence

$$\bar{\pi}_{p,1} = \varepsilon \cdot \pi_{p,1}, \text{ where } \varepsilon \text{ denotes an } m\text{-th root of unity.}$$

Since

$$\tau_{p,1} = \pi_{p,1} + \bar{\pi}_{p,1} = \pi_{p,1}(1+\varepsilon), \text{ and } p = \pi_{p,1} \cdot \bar{\pi}_{p,1}$$

it follows that $(p, \tau_{p,1})$ is divisible by $\pi_{p,1}$. This contradicts to the assumption.

1.3. In the following, we derive a sufficient condition for Q1) to be true. Let $\boldsymbol{K}$ and $\boldsymbol{L}$ be the smallest galois extension fields containing $\boldsymbol{Q}(\tau_{p,1})$ and $\boldsymbol{Q}(\pi_{p,1})$ respectively, we assume the automorphism group *Auto* $(\boldsymbol{K}/\boldsymbol{Q})$ of $\boldsymbol{K}/\boldsymbol{Q}$ is isomorphic to the symmetric group $\mathfrak{S}g$ of order $g!$. The automorphism of $\boldsymbol{L}/\boldsymbol{K}$ induces the transformation $\sqrt{\gamma_i} \to \varepsilon_i \sqrt{\gamma_i}$ with $\varepsilon_i = \pm 1$ $(i=1, \cdots, g)$, where $\gamma_i = \tau_{p,i}^2 - 4p$, whence *Auto* $(\boldsymbol{L}/\boldsymbol{K}) = \mathfrak{H}$ is identified with a subgroup of abelian group $\mathfrak{A}$ of order 2^g and type $(2, 2, \cdots, 2)$ consisting of all combinations $(\varepsilon_1, \cdots, \varepsilon_g)$ of signs ± 1. Since $\mathfrak{H}$ is a normal subgroup of *Auto* $(\boldsymbol{L}/\boldsymbol{Q}) = \mathfrak{G}$, the factor group $\bar{\mathfrak{G}} = \mathfrak{G}/\mathfrak{H}$ $(\cong \mathfrak{S}_g)$ operates on $\mathfrak{H}$ in a canonical way: $T_{\bar{g}}(h) = ghg^{-1}$ for $h \in \mathfrak{H}$, and $\bar{g} = g\mathfrak{H}$. This implies that $\mathfrak{H}$ contains all element $(\varepsilon_{\sigma(1)}, \cdots, \varepsilon_{\sigma(g)})$ together with $h = (\varepsilon_1, \cdots, \varepsilon_g)$ of $\mathfrak{H}$, where $(\sigma(1), \cdots, \sigma(g))$ is a permutation of $(1, 2, \cdots, g)$, whence we can infer without difficulty that $\mathfrak{H}$ is one of the following 4 subgroups of $\mathfrak{A}$.

(1) $\mathfrak{A}_1 = \mathfrak{A}$, the whole group

(2) $\mathfrak{A}_2 = \{(\varepsilon_1, \cdots, \varepsilon_g) \mid \varepsilon_1 \cdot \varepsilon_2 \cdots \varepsilon_g = 1\}$ $\quad [\mathfrak{A}_2 : 1] = 2^{g-1}$

(3) $\mathfrak{A}_3 = \{(1, 1, \cdots, 1), (-1, -1, \cdots, -1)\}$ $\quad [\mathfrak{A}_3 : 1] = 2$

(4) $\mathfrak{A}_4 = \{(1, 1, \cdots, 1)\}$ $\quad [\mathfrak{A}_4 : 1] = 1$

Proposition 2. *The assumption and notations being the same as above,* $\boldsymbol{Q}(\tau_{p,1})$ *is the unique maximal subfield in* $\boldsymbol{Q}(\pi_{p,1}) = \boldsymbol{Q}(\sqrt{\gamma_1})$ *if* $\mathfrak{H} = \mathfrak{A}_1$ *or* $\mathfrak{A}_2$.

Proof. Put, $\boldsymbol{K}_1 = \boldsymbol{Q}(\tau_{p,1})$, $\boldsymbol{L}_1 = \boldsymbol{Q}(\sqrt{\gamma_1}) = \boldsymbol{Q}(\pi_{p,1})$. First we shall show $\boldsymbol{K} \cap \Phi = \boldsymbol{Q}$ for any subfield $\Phi \neq \boldsymbol{Q}$ of L_1 which is not contained in K_1.

Since $\mathfrak{S}_{g-1}(\cong Auto\,(K/K_1))$ is a maximal subgroup of $\mathfrak{S}_g$, $K_1/\boldsymbol{Q}$ does not contain any proper subfield. We have, on the other hand, $L_1\cap K=K_1$. Therefore $K\cap\Phi=K\cap(\Phi\cap L_1)=(K\cap L_1)\cap\Phi=K_1\cap\Phi=\boldsymbol{Q}$. Let $\mathfrak{L}$ be the automorphism group $Auto(\boldsymbol{L}/\boldsymbol{\Phi})$. Since $K\cap\Phi=\boldsymbol{Q}$, we have $\mathfrak{L}\mathfrak{H}=\mathfrak{G}$ We put $M=\Phi\cdot K=\Phi K_1\cdot K=L_1\cdot K$. Then $[M:K]=[L_1\cdot K:K]=2$, and so $[\mathfrak{H}:Auto(L/M)]=2$. We put $\mathfrak{H}_1=Auto(L/M)$. Then $\mathfrak{H}_1=\mathfrak{H}\cap\mathfrak{L}$, hence $\mathfrak{H}_1$, is a normal abelian subgroup of $\mathfrak{L}$ and so $\mathfrak{H}_1$ has $\mathfrak{S}_g\cong\mathfrak{G}/\mathfrak{H}=\mathfrak{L}\mathfrak{H}/\mathfrak{H}$ $=\mathfrak{L}/\mathfrak{L}\cap\mathfrak{H}=\mathfrak{L}/\mathfrak{H}_1$ as an operator group. One finds however, that there does not exist such a subgroup $\mathfrak{H}_1$ in $\mathfrak{H}$ because any element of $\mathfrak{H}_1$ must fix $\sqrt{\gamma_1}$. This completes the proof.

The assumption that $\mathfrak{L}_i=\boldsymbol{Q}(\sqrt{\gamma_i})$ is totally imaginary of degree $2g$ over $\boldsymbol{Q}$ implies $\mathfrak{H}\neq\mathfrak{A}_4$. If $\mathfrak{H}=\mathfrak{A}_4$, then $K=L\supset L_i$, and so L_i is a subfield of the totally real number field K. This contradicts to the assumption on L_i.

If $\mathfrak{H}=\mathfrak{A}_3$, then $K(\sqrt{\gamma_1})=K(\sqrt{\gamma_2})=\cdots=K(\sqrt{\gamma_g})=L$, and hence $\sqrt{\gamma_i\gamma_j}\in K$, $i,j=1,\cdots,g$. $\xi_{ij}=\gamma_i\gamma_j\ (i\neq j)$ is contained in the subfield K' of K corresponding to a subgroup isomorphic to $\mathfrak{S}_2\times\mathfrak{S}_{g-2}$, where K' has the degree $\dfrac{g!}{2!(g-2)!}=\dfrac{g(g-1)}{2}=g'$ over $\boldsymbol{Q}$. Therefore $N_{K'/\boldsymbol{Q}}(\gamma_i\gamma_j)=(N_{K_1/\boldsymbol{Q}}(\gamma_1))^{g-1}$. We put then

$$(1)\qquad K'(\sqrt{\xi_{12}})=K'$$

$$(2)\qquad K'(\sqrt{\xi_{12}})=K'(\sqrt{\gamma'})\ (\subseteqq K)\ \text{for some}\ \gamma\in K'.$$

If (1) holds, then $\xi_{12}=\beta_{12}^2$ for some $\beta_{12}\in K'$; hence, defining a polynomial $F(x)\in\boldsymbol{Z}[x]$ by $F(x)=\Pi(x-\xi_{ij})$ we have a facotorization $F(x^2)=\pm\Phi(x)\times\Phi(-x)$ with $\Phi(x)=\Pi(x-\beta_{ij})\in\boldsymbol{Z}[x]$. Putting $F(x^2)=x^{2g'}-a_1x^{2(g'-1)}+\cdots+(-1)^{g'}a_{g'}$, $\Phi(x)=x^{g'}-b_1g'+\cdots+(-1)^{g'}b_{g'}$, we have g' equations in a_i, b_j with integral coefficients. If these g' eqations do not have any integral solutions, then we can conclude $\mathfrak{H}\neq\mathfrak{A}_3$. (This is the case in particular, if a_g $(=N_{K'/\boldsymbol{Q}(\xi_{12})})$, is not the square of rational number.) If (2) holds, then. $N_{K'/\boldsymbol{Q}}\left(\dfrac{\xi_{12}}{\gamma}\right)$ must be a square of any rational number. Therefore if $N_{K'/\boldsymbol{Q}}\left(\dfrac{\xi_{12}}{\gamma}\right)$ is not square of any rational number, then $\mathfrak{H}\neq\mathfrak{A}_3$.

2. Numerical examples. In this section we apply the above results to $\Gamma_0(41)$, $\Gamma_0(47)$. For this purpose, we determine the characteristic equation of T_p acting on $S_{-2}(\Gamma_0(41))$, $S_{-2}(\Gamma_0(47))$, the spaces of cusp form of degree -2 corresponding to the modular groups $\Gamma_0(41)$, and $\Gamma_0(47)$ respectively, by calculating traces $Sp(T_p^m)$ of the powers of these T_p.

Lemma. *The characteristic equations of T_p with respect to $S_{-2}(\Gamma_0(N))$*

are as follows. In the case; the dimension of $J_{\Gamma_0(N)}$ *is* 3:

$$X^3 - Sp(T_p)X^2 + \frac{Sp^2(T_p) - Sp(T_p^2)}{2}X - \frac{(Sp^3(T_p) + Sp(T_p^3) - 2Sp(T_p)Sp(T_p^2))}{6} = 0$$

In the case; the dimension of $J_{\Gamma_0(N)}) = {}_{\Gamma_0(N)}$ is 4:

$$X^4 - Sp(T_p)X^3 + \frac{Sp^2(T_p) - Sp(T_p^2)}{2}X^2 - \frac{[Sp^3(T_p) + 2Sp(T_p^3) - 3Sp(T_p)Sp(T_p^2])}{6}X$$
$$+ \frac{Sp(T_p)Sp(T_p^3)}{3} - \frac{[Sp^2(T_p)Sp(T_p^2) + Sp(T_p^4)]}{4} + \frac{Sp^2(T_p^2)}{8} + \frac{Sp(T_p)}{24} = 0$$

Proof. It follows by the simple calculation as the same method as in [1; lemma 1].

Using the trace-formula [2], we get the following table of traces $Sp(T_p^m)$:

	genus	$Sp(T_5)$	SpT_5^2	SpT_5^3	SpT_5^4	SpT_5^2	SpT_5^3	SpT_5^4	SpT_7	SpT_7^2	SpT_7^3	SpT_7^2	SpT_7^3
$\Gamma_0(41)$	3	-2	-3	0		12	-20		-6	-1	-18	20	66
$\Gamma_0(47)$	4	-2	16	-36	24	36	-56	464					

The characteristic equations of T_5 and T_7 with respect to $S_{-2}(\Gamma_0(41))$ are $X^3 + 2X^2 - 4X - 4 = 0$ and $X^3 - 6X^2 + 8X - 2 = 0$ respectionaly, and that of T_5 with respect to $S_{-2}(\Gamma_0(49))$ is $X^4 + 2X^3 - 16X^2 - 16X + 48 = 0$. These equations are irreducible over $\boldsymbol{Q}$. Let $\boldsymbol{K}$, $\boldsymbol{K}'$, $\boldsymbol{K}''$ be respectively the smallest galois extension fields containing $\boldsymbol{Q}(\tau_{5,1})$, $\boldsymbol{Q}(\tau_{7,1})$ and $\boldsymbol{Q}(\eta_{5,1})$, where $\tau_{5,1}^3 + 2\tau_{5,1}^2 - 4\tau_{5,1} - 4 = 0$, $\tau_{7,1}^3 - 6\tau_{7,1}^2 + 8_{7,1} - 2 = 0$, $\eta_{5,1}^4 + 2\eta_{5,1}^3 - 16\eta_{5,1}^2 - 16\eta_{5,1} + 48 = 0$. Then we know by simple calculation that the galois groups of $\boldsymbol{K}$, $\boldsymbol{K}'$ are both isomorphic to the symmetric group $\mathfrak{S}_3$ of order 3! and that of K'' is isomorphic to $\mathfrak{S}_4$ of order 4!.

Case $\Gamma_0(41)$, T_5, if (1) in 1.3 holds, there should be the following relations among the coefficients b_i of $\Phi(x)$ and the a_i of $F(x)$ ($\gamma_i = \tau_{5,1}^2 - 20$ $(i=1, 2, 3)$, $\xi_{ij} = \gamma_i \cdot \gamma_j$ and $F(x) = \prod_{i,j}(x - \xi_{ij}) = x^3 - a_1x^2 + a_2x - a_3$: $2b_2 - b = 752 = 2^4 \cdot 47$, $b_2^2 - 2b_1b_3 = 172866$, $b_3^2 = -2^4 \cdot 239$ While the corresponding relations for J_7 are $2b_2 - b_1^2 = 2^2 \cdot 5^2 \cdot 37$, $b_2^2 - 2b_1b_3 = 2^6 \cdot 13 \cdot 1667$, $b_3^2 = -2^4 \cdot 239$). However, these equations do not have any rational solution b_i. If (2) in 1.3 hold, $\boldsymbol{Q}(\tau_{5,1})(\sqrt{\xi_{12}}) = K = \boldsymbol{Q}(\tau_{5,1})(\sqrt{D})$, where $D(=2^4 \cdot 37)$ is the discriminant of the equation $X^3 + 2X^2 - 4X - 4 = 0$. Then $N_{\boldsymbol{Q}(\tau_{5,1})/\boldsymbol{Q}}\left(\frac{\xi_{12}}{D}\right)$ must be a square of a rational number. But we get $N_{\boldsymbol{Q}(\tau_{5,1})/\boldsymbol{Q}}\left(\frac{\xi_{12}}{D}\right) = \frac{N_{\boldsymbol{Q}(\tau_{5,1})}(\gamma_1)^2}{D^3} = \frac{(2^4 \cdot 239)^2}{2^{12} \cdot 37^3}$. Therefore $\mathfrak{H} \neq \mathfrak{A}_3$. Obviously $\mathfrak{H} \neq \mathfrak{A}_4$ ($[L:K] \neq 1$).

This, together with Proposition 2, shows that $\boldsymbol{Q}(\tau_{5,1})$ is the unique maximal subfield in $\boldsymbol{Q}(\tau_{5,1})$. By an analogous argument we see also that $\boldsymbol{Q}(\tau_{7,1})$ is the unique maximal subfield in $\boldsymbol{Q}(\pi_{7,1})$. Thus, for the case of $\Gamma(41)$, the conditions of criterion (B) are whole satisfied

$$5 \not| 6 \cdot 41 \ (7 \not| 6 \cdot 41)$$

P1) $[\boldsymbol{Q}(\tau_{5,1}):\boldsymbol{Q}] = 3 \quad ([\boldsymbol{Q}(\tau_{7,1}):\boldsymbol{Q}] = 3)$

P2′) $[\boldsymbol{Q}(\pi_{5,1}):\boldsymbol{Q}] = 6 \quad ([\boldsymbol{Q}(\pi_{7,1}):\boldsymbol{Q}] = 6)$

Q1) $\boldsymbol{Q}(\tau_{5,1})$ $(\boldsymbol{Q}(\tau_{7,1}))$ is the unique maximal subfield in $\boldsymbol{Q}(\pi_{5,1})(\boldsymbol{Q}(\pi_{7,1}))$

Q2′) $(N_{(\tau_{5,1})/\boldsymbol{Q}}(\tau_{5,1}),\ 5) = (4, 5) = 1$

$(N_{(\tau_{7,1})/\boldsymbol{Q}}(\tau_{7,1}),\ 7) = (2, 7) = 1)$

Hence $\mathcal{A}_0(J_{\Gamma_0(41)}) \subset \mathcal{A}_0(\tilde{J}_{\Gamma_0(41)} \bmod 5) \cong \boldsymbol{Q}(\pi_{5,1})$

and $\mathcal{A}_0(J_{\Gamma_0(41)}) \subset \mathcal{A}_0(\tilde{J}_{\Gamma_0(41)} \bmod 7) \cong \boldsymbol{Q}(\pi_{7,1})$.

Moreover, we have in this case, $\tau_{5,1}=4\tau_{7,1}-\tau_{7,1}^2-2$ which implies $\boldsymbol{Q}(\tau_{5,1})=\boldsymbol{Q}(\tau_{7,1})$, while $\boldsymbol{Q}(\pi_{5,1})\neq\boldsymbol{Q}(\pi_{7,1})$ because we have $N_{\boldsymbol{Q}(\tau_{5,1})/\boldsymbol{Q}}\left(\frac{\tau_{2,1}^5-20}{\tau_{7,1}^2-28}\right)=\frac{2^2\cdot 239}{1847}$. Therefore $\mathcal{A}_0(J_{\Gamma_0(41)})\cong\boldsymbol{Q}(\tau_{5,1})$.

Case $\Gamma_0(47)$, T_5 : $N_{k_0/\boldsymbol{Q}}(\xi_{12})=(N_{\boldsymbol{Q}(\eta_{5,1}/\boldsymbol{Q})}(\gamma_1))^{4-1}=[N_{\boldsymbol{Q}(\eta_{5,1})/\boldsymbol{Q}}(\eta_{5,1}^2-20)]^3=(2^{10}\cdot 23\cdot 5)^3$, ie ξ_{12} is not *a* square of any element β of $\boldsymbol{K}_0=\boldsymbol{Q}(\xi_{12})$, where $[\boldsymbol{K}_0:\boldsymbol{Q}]=6\left(=g'=\frac{g(g-1)}{2}\right)$. Hence

(1) in 1.3 does not hold. Let us now assume the condition (2) in 1.3. We have then $[K_0(\sqrt{\xi_{12}}):K_0]=2$. Since in this case $Auto\,(K/K_0)\cong\{1, (12), (34), (12)(34)\}\subset\mathfrak{S}_4$, we have

$$Auto\,(K/K_0(\sqrt{\xi_{12}})) \cong \{1, (12)\} \cdots\cdots\cdots (\text{i})$$

or $\cong \{1, (34)\} \cdots\cdots\cdots (\text{ii})$

or $\cong \{1, (12)(34)\} \cdots (\text{iii})$,

where

$$(\text{i}) \Rightarrow K_0(\sqrt{\xi_{12}}) = K_0(\eta_{5,1}\eta_{5,2}(\eta_{5,3}-\eta_{5,4})) = K_0(\sqrt{\eta_{5,1}^2\eta_{5,2}^2(\eta_{5,3}-\eta_{5,4})^2})$$

$$(\text{ii}) \Rightarrow K_0(\sqrt{\xi_{12}}) = K_0(\eta_{5,1}-\eta_{5,2})(\eta_{5,3}\eta_{5,4}) = K_0(\sqrt{(\eta_{5,1}-\eta_{5,2})^2\eta_{5,3}^2\eta_{5,4}^2})$$

$$(\text{iii}) \Rightarrow K_0(\sqrt{\xi_{12}}) = K_0(\eta_{5,1}-\eta_{5,2}((\eta_{5,3}-\eta_{5,4})) = K_0(\sqrt{\eta_{5,1}-\eta_{5,2})^2(\eta_{5,3}-\eta_{5,4})^2}$$

Therefore $N_{k_0/\boldsymbol{Q}}\left(\frac{\xi_{12}}{\eta_{5,1}^2\eta_{5,2}^2(\eta_{5,3}-\eta_{5,4})^2}\right)$,

$N_{k_0/\boldsymbol{Q}}\left(\frac{\xi_{12}}{(\eta_{5,1}-\eta_{5,2})^2\eta_{5,3}^2\eta_{5,4}^2}\right)$ and

$N_{k_0/Q}\left(\dfrac{\xi_{12}}{(\eta_{5,1}-\eta_{5,2})^2(\eta_{5,3}-\eta_{5,4})^2}\right)$ must be squares of rational numbers. In our case however,

$$N_{k_0/Q}\left(\frac{\xi_{12}}{\eta_{5,1}^2\eta_{5,2}^2(\eta_{5,3}-\eta_{5,4})^2}\right)=N_{k_0/Q}\left(\frac{\xi_{12}}{(\eta_{5,1}-\eta_{5,2})^2\eta_{5,3}^2\eta_{5,4}^2}\right)=\frac{2^{30}\cdot 23^3\cdot 5^3}{2^{24}\cdot 3^6\cdot 2^2\cdot 89501\cdot 23}$$

$$N_{k_0/Q}\left(\frac{\xi_{12}}{(\eta_{5,1}-\eta_{5,2})^2(\eta_{5,3}-\eta_{5,4})^2}\right)=\frac{2^{30}\cdot 23^3\cdot 5^3}{2^4\cdot 89501^2\cdot 23^2},$$

hence (2) does not hold. Hence $\mathfrak{H}\neq\mathfrak{A}_3$. We have further $(\eta_{5,1}, 5)=(N_{Q(\eta_{5,1})/Q}(\eta_{5,1}), 5)=(48, 5)=1$. By Proposition 2 and Criterion (B), $(\mathcal{A}_0\tilde{J}_{\Gamma_0(47)} \bmod 5)\cong \boldsymbol{Q}(\pi_{5,1})$. Therefore $\tilde{J}_{\Gamma_0(47)}$ is simple, and so is $J_{\Gamma_0(47)}$ simple.

OSAKA CITY UNIVERSITY

References

[1] K. Doi: *On the jacobian varieties of the fields of elliptic modular functions,* Osaka Math. J. **15** (1963) 249–256.

[2] M. Eichler: *Über die Darstellbarkeit von Modulformen durch Thetareihen,* J. Reine Angew. Math. **195** (1956), 156–171.

[3] G. Shimura: *Correspondences modulaires et les fonctions de courbe algébriques,* J. Math. Soc. Japan **10** (1958), 1–28.

[4] G. Shimura and Y. Taniyama: Complex multiplication of abelian varieties and its applications to number theory, Publ. Math. Soc. Japan, No. 6, 1961.