J. Math. Kyoto Univ.
6-2 (1967) 177-185

On the jacobian varieties of the fields of elliptic modular functions II.

By

Koji Doi* and Hidehisa Naganuma

(Roceived November 29, 1966)

The purpose of this note is to observe the Galois groups of normal extensions obtained by the coordinates of the ideal section points of the jacobian variety J_q of an algebraic curve uniformized by elliptic modular functions, which was investigated in a previous work [2] with the same title. Our result can be obtained by slight modification of the consideration due to G. Shimura [6]. In fact, in his [6, footnote 9), p. 281], our problem was suggested.

In §4 of the present paper, we treated a simple jacobian variety J_q of dimension 2, having a real quadratic number field $\boldsymbol{Q}(\sqrt{d})$ as its endomorphism algebra. By a numerical example, we shall show that there occur two types of Galois group $G(K(\mathfrak{l})/\boldsymbol{Q})$, according as $\left(\frac{d}{l}\right)=+1$ or -1, which is isomorphic to $GL(2, GF(l))$ or $GF(l)^{*}\cdot SL(2, GF(l^2))$ respectively, where $\mathfrak{l}$ $(\mid l)$ denotes a prime ideal in $\boldsymbol{Q}$ $(\sqrt{d})$ and $K(\mathfrak{l})/\boldsymbol{Q}$ a normal extension generated by the coordinates of the $\mathfrak{l}$-section points of J_q.

Notations. Let F be an algebraic number field of finite degree over $\boldsymbol{Q}$ and $\mathfrak{o}$ be the ring of integers in F. Let (A^n, θ) be an abelian variety of type (F) in the sense of [4] i.e. a couple (A, θ) formed by an abelian variety A of the dimension n and an isomorphism θ of F into $\mathrm{End}_{\boldsymbol{Q}} A = \mathrm{End}\, A \otimes_{\boldsymbol{Z}} \boldsymbol{Q}$ such that $\theta(1)=1_A$ (=the identy element of $\mathrm{End}_{\boldsymbol{Q}} A$). In the following treatment, (A^n, θ) will denote

* This work was partially supported by The Sakkokai Foundation.

an abelian variety of type (F) which are assumed to be principal, namely, we assume that $\theta(\mathfrak{o})=\mathrm{End}_{\boldsymbol{Q}}A\cap\theta(F)$. Putting $m=2n/[F:\boldsymbol{Q}]$ for (A^{n},θ), m is called the index of (A^{n},θ). For a prime ideal $\mathfrak{l}$ of $\mathfrak{o}$ and a natural number ν, put

$$\mathfrak{g}(\mathfrak{l}^{\nu},A)=\{t\in A\,|\,\theta(a)t=0 \text{ for all } a\in\mathfrak{l}^{\nu}\},\quad \mathfrak{g}(\mathfrak{l}^{\infty},A)=\bigcup_{\nu=1}^{\infty}\mathfrak{g}(\mathfrak{l}^{\nu},A).$$

§1. $\mathfrak{l}$-adic representation $M_{\mathfrak{l}}$.

Let (A^{n},θ) be an abelian variety type (F) with the index m. For a prime ideal $\mathfrak{l}$ of $\mathfrak{o}$ which is prime to the characteristic of the field of definition for A, we have

$$(1\cdot 1)\qquad \begin{aligned}&\mathfrak{g}(\mathfrak{l}^{\nu},A)\cong\mathfrak{o}/\mathfrak{l}^{\nu}\oplus\cdots\oplus\mathfrak{o}/\mathfrak{l}^{\nu}\ (m\text{-copies})\\ &\mathfrak{g}(\mathfrak{l}^{\infty},A)\cong F_{\mathfrak{l}}/\mathfrak{o}_{\mathfrak{l}}\oplus\cdots\oplus F_{\mathfrak{l}}/\mathfrak{o}_{\mathfrak{l}}\ (m\text{-copies}),\end{aligned}$$

where $F_{\mathfrak{l}}$ and $\mathfrak{o}_{\mathfrak{l}}$ denotes the $\mathfrak{l}$-completion of F and the valuation ring in $F_{\mathfrak{l}}$, respectively. We call any one of the isomorphisms of $\mathfrak{g}(\mathfrak{l}^{\infty},A)$ onto $\overset{m}{\bigoplus}F_{\mathfrak{l}}/\mathfrak{o}_{\mathfrak{l}}$ an $\mathfrak{l}$-adic coordinate-system of $\mathfrak{g}(\mathfrak{l}^{\infty},A)$ and choose a fixed one, say, $\mathfrak{v}$, Let $Z(A,F)$ and $Z_0(A,F)$ denotes the commutator of $\theta(\mathfrak{o})$ in End A and of $\theta(F)$ in $\mathrm{End}_{\boldsymbol{Q}}(A)$, respectively. Then for an element $\lambda\in Z(A,F)$, there exists a square matrix M of size m, with coefficients in $\mathfrak{o}_{\mathfrak{l}}$, such that, for every $t\in\mathfrak{g}(\mathfrak{l}^{\infty},A)$, we have $\mathfrak{v}(\lambda t)=M\mathfrak{v}(t)$. The mapping $\lambda\to M$ is uniquely extended to a representation of $Z_0(A,F)$ by matrices with coefficients in $F_{\mathfrak{l}}$, which we call the $\mathfrak{l}$-adic representation of $Z_0(A,F)$ with respect to $\mathfrak{v}$. For an element $\xi\in Z_0(A,F)$ and an $\mathfrak{l}$-adic representation $M_{\mathfrak{l}}$ of $Z_0(A,F)$, we denote by $P_{\mathfrak{l}}(\xi,X)$ the characteristic polynomial of $M_{\mathfrak{l}}(\xi)$ i.e.,

$$\det\,(X\cdot 1_m-M_{\mathfrak{l}}(\xi))=P_{\mathfrak{l}}(\xi,X),$$

where X is an indetermicate and 1_m denotes the unit matrix of size m.

Let (A,θ) be an abelian variety of type (F), defined over k, which is principal. Namely, k is a field of definition for A and every element of $\theta(\mathfrak{o})$. We denote by $\mathrm{End}(A,k)$ the set of all elements in $\mathrm{End}(A)$ defined over k. In the present treatment we restrict ourselves to the case where k is an algebraic number field and we recall a few facts in [4], which concerns the reduction of abelian variety with respect to a discrete place $\mathfrak{p}$ of k. We denote by $\tilde{k}$ the residue field of k with respect to $\mathfrak{p}$. (A, θ) being as above, then, if A has no defect for $\mathfrak{p}$, $(A_{\mathfrak{p}}, \tilde{\theta})$ is principal, where $A_{\mathfrak{p}}$ is the reduction of A modulo $\mathfrak{p}$ and $\tilde{\theta}(\mu)=\widetilde{\theta(\mu)}$ (=the reduction of $\theta(\mu)$ modulo $\mathfrak{p}$) for every $\mu \in \mathfrak{o}$. For every $\lambda \in \mathrm{End}(A, k)$ and its reduction $\tilde{\lambda}$ of λ modulo $\mathfrak{p}$, the correspondence $\lambda \rightarrow \tilde{\lambda}$ defines a ring-isomorphism of $\mathrm{End}(A, k)$ into $\mathrm{End}(A_{\mathfrak{p}}, \tilde{k})$. Let $\mathfrak{l}$ be a prime ideal of $\mathfrak{o}$ which is prime to the characteristic of $\tilde{k}$. We can choose $\mathfrak{l}$-adic coordinate systems of $\mathfrak{g}(\mathfrak{l}^{\infty}, A)$ and $\mathfrak{g}(\mathfrak{l}^{\infty}, A_{\mathfrak{p}})$ in such a way that for every $\lambda \in \mathrm{End}(A, k)$, we have $M_{\mathfrak{l}}(\lambda)=M_{\mathfrak{l}}(\tilde{\lambda})$. For every integral ideal $\mathfrak{a}$ of F, the reduction modulo $\mathfrak{p}$ defines a homomorphism of $\mathfrak{g}(\mathfrak{a}, A)$ onto $\mathfrak{g}(\mathfrak{a}, A_{\mathfrak{p}})$, provided that every point of $\mathfrak{g}(\mathfrak{a}, A)$ is rational over k. Moreover, if $\mathfrak{a}$ is prime to the characteristic of $\tilde{k}$, this homomorphism is an isomorphism. We remark that the $N(\mathfrak{p})$-th power endomorphism $\pi_{\mathfrak{p}}$ is contained in $Z(A_{\mathfrak{p}}, F)$ since (A, θ) is assumed to be defined over k.

§2. Galois group $G(K(\mathfrak{l})/k)$.

Let (A, θ) be an abelian variety of type (F), defined over an algebraic number field k of finite degree, which is principal. For a prime ideal $\mathfrak{l}$ of $\mathfrak{o}$ and a natural number n, let $K(\mathfrak{l}^n)$ resp. $K(\mathfrak{l}^{\infty})$ be the field generated over k by the coordinates of the points in $\mathfrak{g}(\mathfrak{l}^n, A)$ resp. in $\mathfrak{g}(\mathfrak{l}^{\infty}, A)$. The field $K(\mathfrak{l}^n)$ resp. $K(\mathfrak{l}^{\infty})$ is a finite resp. an infinite normal extension of k. Taking a basis of $\mathfrak{g}(\mathfrak{l}^n, A)$ resp. $\mathfrak{g}(\mathfrak{l},^{\infty} A)$, we get a representation $R^{\mathfrak{l}}{}_n$ resp. $R^{\mathfrak{l}}{}_{\infty}$ of the Galois group $G(K(\mathfrak{l}^n)/k)$ resp. $G(K(\mathfrak{l}^{\infty})/k)$ by matrices in $GL(m, \mathfrak{o}/\mathfrak{l}^n)$ resp. $GL(m, \mathfrak{o}_{\mathfrak{l}})$ by means of (1.1), where m is the index of (A, θ). We may assume that

$$R^{\mathfrak{l}}{}_n(\sigma') \equiv R^{\mathfrak{l}}{}_{\infty}(\sigma) \mod (\mathfrak{l}^n)$$

if σ' is the restriction of an element σ of $G(K(\mathfrak{l}^{\infty})/k)$ to $K(\mathfrak{l}^n)$.

Let $\mathfrak{p}$ be a prime ideal of k, for which we assume that A has no defect and let $\mathfrak{P}$ be a prime divisor of $\mathfrak{p}$ in $K(\mathfrak{l}^\infty)$, and $\mathfrak{P}'$ the restriction of $\mathfrak{P}$ to $K(\mathfrak{l}^n)$. Let $\sigma_{\mathfrak{P}}$ be a Frobenius automorphism for $\mathfrak{P}$. The restriction σ' of $\sigma_{\mathfrak{P}}$ to $K(\mathfrak{l}^n)$ is a Frobenius automorphism for $\mathfrak{P}'$. As was remarked in §1, the reduction modulo $\mathfrak{P}$ defines an isomorphism of $\mathfrak{g}(\mathfrak{l}^\infty, A)$ onto $\mathfrak{g}(\mathfrak{l}^\infty, A_{\mathfrak{p}})$, provided that $\mathfrak{l}$ is prime to the characteristic of $\widetilde{k}$. From the definition of Frobenius automorphism, we see that

$$t^\sigma \bmod \mathfrak{P} = \pi_{\mathfrak{p}}(t \bmod \mathfrak{P}) \quad (t \in \mathfrak{g}(\mathfrak{l}^\infty, A)).$$

Therefore, choosing suitable basis of $\mathfrak{g}(\mathfrak{l}^\infty, A)$ and $\mathfrak{g}(\mathfrak{l}^\infty, A_{\mathfrak{p}})$, we get $R^{\mathfrak{l}}_\infty(\sigma_{\mathfrak{P}}) = M_{\mathfrak{l}}(\pi_{\mathfrak{p}})$, so that

$$\det[X\cdot 1_m - R^{\mathfrak{l}}_\infty(\sigma_{\mathfrak{P}})] = P_{\mathfrak{l}}(\pi_{\mathfrak{p}}, X)$$
$$\det[X\cdot 1_m - R^{\mathfrak{l}}_n(\sigma')] \equiv P_{\mathfrak{l}}(\pi_{\mathfrak{p}}, X) \bmod \mathfrak{l}^n.$$

For the determination of $G(K(\mathfrak{l})/k)$ in the special case of (A,θ) as in §4, we shall need the following statement concerning the representation $R^{\mathfrak{l}}_1 : G(K(\mathfrak{l})/k) \to GL(m, \mathfrak{o}/\mathfrak{l})$. This is a special case of a more precise result due to Shimura [5].

Proposition 1. *Let F be a totally real algebraic number field of finite degree and (A,θ) an abelian variety of type (F), defined over $\boldsymbol{Q}$, which is principal and of index m. Suppose that $\theta(F) = \mathrm{End}_{\boldsymbol{Q}}(A)$. Then we have*

$$R^{\mathfrak{l}}_1[G(K(\mathfrak{l})/\boldsymbol{Q})] \subset (\boldsymbol{Z}/c)^* \cdot SL(m, \mathfrak{o}/\mathfrak{l}),$$

where c is the smallest positive integer divisible by $\mathfrak{l}$, and $(\boldsymbol{Z}/c)^*$ denotes the multiplicative group in $\boldsymbol{Z}/c$.

Proof. Let C be a polarization of A. We remark that the automorphism group of the polarized abelian variety (A, C, θ) is $\{\pm 1\}$. Then the proof is included in [5, Th. 7.2, p. 150].

§3. Jacobian variety J_q.

For every positive integer q, put

$$\Gamma_0(q) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2, \boldsymbol{Z}) \mid c \equiv 0 (q) \right\}.$$

Then $\Gamma_0(q)$ is a properly discontinuous group operating on the upper half plane

$$H=\{z\in \boldsymbol{C}\,|\,I_m(z)>0\}.$$

Let C_q be a non-singular curve of the field of modular functions belonging to the group $\Gamma_0(q)$, and J_q the jacobian variety of C_q. Let T_p be the element of $\mathrm{End}_{\boldsymbol{Q}}(J_q)$, corresponding to the so called Hecke operator acting on the space $S_2(\Gamma_0(q))$ of cusp forms of weight 2 with respect to $\Gamma_0(q)$. We can take $\boldsymbol{Q}$ as the field of definition for C_q, J_q and T_p. For every prime number p, other than $p\,|\,q$, we have "good" reduction modulo p for C_q, J_q and the so called congruence relation

$$\widetilde{T}_p=\pi_p+\pi'_p, \tag{3.1}$$

where π_p is the p-th power endomorphism of $(J_q)_p$ (=reduction of J_q modulo p), $\pi'_p=p\cdot\pi_p^{-1}$ and $\widetilde{T_p}$ is the reduction of T_p modulo p. Let M^d be a representation of $\mathrm{End}_{\boldsymbol{Q}}(J_q)$ by the differential forms of the first kind, then $M^d(T_p)$ can be considered as a representation of T_p for the space $S_2(\Gamma_0(q))$. It is well-known that the eigenvalues of $M^d(T_p)$ are real algebraic integers of finite degree$\leqslant g$(=the genus of C_q). Taking an eigenvalue c_p of $M^d(T_p)$ and putting $\theta(c_p)=T_p$, we get an abelian variety (J_q^g,θ) of type $(\boldsymbol{Q}(c_p))$.

In certain cases, the jacobian variety J_q^g turns out to be simple and $\mathrm{End}_{\boldsymbol{Q}}(J_q)$ is generated by T_n over $\boldsymbol{Q}$, which is isomorphic to a totally real algebraic number field of degree g (*cf.* [2], [3]). We shall determine the galois Groups $G(K(\mathfrak{l})/\boldsymbol{Q})$ for some $\mathfrak{l}$, in §4, in a special case of these. For these reasons, we restrict ourselves to the following situations.

Now let us consider the jacobian variety (J_q,θ) under the conditions such that (J_q,θ) is principal and of index 2, which is defined over $\boldsymbol{Q}$ and $T_n\in\theta(F)$ for every natural number n, where F is a totally real algebraic number field. Let $\mathfrak{o}$ be the ring of integers in F and $\mathfrak{l}$ a prime ideal of $\mathfrak{o}$. As we defined in §1, $P_{\mathfrak{l}}(\pi_p, X)$ denotes the characteristic polynomial of $M_{\mathfrak{l}}(\pi_p)$, where π_p in the p-th power endomorphism of $(J_q)_p$.

Proposition 2. *Let (J_q, θ) be the jacobian variety satisfying the above conditions. Let p be a prime number such that $p \nmid q$, and $\mathfrak{l}$ a prime ideal in F which is prime to p. Then the characteristic polynomial $P_{\mathfrak{l}}(\pi_p, X)$ is given by*

$$P_{\mathfrak{l}}(\pi_p, X) = X^2 - c_p X + p,$$

either the condition (A) or (B) is satisfied:

(A) $c_p^2 - 4p = \mathfrak{l}\cdot\mathfrak{m}$ *(in $\mathfrak{o}$) where* $(\mathfrak{l}, \mathfrak{m}) = 1$.

(B) $X^2 \equiv c_p^2 - 4p$ $(\mathfrak{l})$ *has no solutions in $\mathfrak{o}$ i.e $c_p^2 - 4p$ is not a quadratic residue mod. $\mathfrak{l}$.*

In particular, if (A) is satisfied, $R^{\mathfrak{l}}{}_1(\sigma')$ is conjugate to $\begin{pmatrix} b & 1 \\ 0 & b \end{pmatrix}$.

Proof. The first part of our assertion is an easy consequence of (3.1) i.e., $\pi_p^2 - \pi_p T_p + p\cdot\delta_{(J_q)_p} = 0$, where $\delta_{(J_q)_p}$ is the identity automorphism of $(J_q)_p$. This means that

$$(M_{\mathfrak{l}}(\pi))^2 - M_{\mathfrak{l}}(\pi)\cdot\begin{pmatrix} c_p & 0 \\ 0 & c_p \end{pmatrix} + \begin{pmatrix} p & 0 \\ 0 & p \end{pmatrix} = 0.$$

If we put $M_{\mathfrak{l}}(\pi_p) = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$, $\alpha, \beta, \gamma, \delta \in \mathfrak{o}_{\mathfrak{l}}$, it follows

$$\alpha^2 - c_p\alpha + p + \beta\gamma = 0$$
$$\delta^2 - c_p\alpha + p + \beta\gamma = 0$$
$$\beta(\alpha + \delta - c_p) = 0$$
$$\gamma(\alpha + \delta - c_p) = 0.$$

This shows that $P_{\mathfrak{l}}(\pi_p, X) = X^2 - c_p X + p$, except for the case $M_{\mathfrak{l}}(\pi_p) = \begin{pmatrix} \omega & 0 \\ 0 & \omega \end{pmatrix}$, where $\omega = c_p \pm \sqrt{c_p^2 - 4p}/2$. However, our assumption (A) or (B) means $c_p^2 - 4p \notin F_{\mathfrak{l}}$. Hence, if either (A) or (B) is satisfied the exceptional case does not occur. The second part of our assertion follows from the same argument as the proof of [6, Lemma 1, p.213].

§4. The case of $\Gamma_0(23)$.

Let us consider the special case $q = 23$ (= the smallest prime number for which C_q is of genus 2). We denote, as usual, by $\Delta(z)$ the cusp-form of degree 12 with respect to $SL(2, \boldsymbol{Z})$ and put

$$f(z)=\sqrt[12]{\Delta(z)\cdot\Delta(23z)}=\sum_{n=1}^{\infty} a_n q^n;\ q=e^{2\pi iz}$$
$$g(z)=T_2(f(z)).$$

Then $f(z), g(z)$ is one of the basis of $S_2(\Gamma_0(23))$. Furthermore, if we put

$$\varphi_i(z)=g(z)+\alpha_i\cdot f(z)=\sum_{n=1}^{\infty} c_{n,i}q^n;\ i=1,2,$$

so that the corresponding Dirichlet series $\sum_n c_{n,i}n^{-s}$ should admit an Euler product, it can be verified that α_i satisfies $\alpha_i^2-\alpha_i-1=0$ and the eigenvalues $c_{p,i}$ of Hecke operators T_p are given by

$c_{p,1}=a_{2p}+\dfrac{1+\sqrt{5}}{2}a_p$ and $c_{p,2}=a_{2p}+\dfrac{1-\sqrt{5}}{2}a_p$, especially,

$c_{2,1}=\dfrac{-1+\sqrt{5}}{2}$.

In this case (J_{23}, θ) is a simple abelian variety of dimension 2 (*cf.* [2]) so that the situations of Proposition 1 and that of §3 are applicable. Namely, $\theta(c_{p,1})=T_p$ gives an isomorphism of $\boldsymbol{Q}(\sqrt{5})$ onto $\mathrm{End}_{\boldsymbol{Q}}(J_{23})$ and (J_{23}, θ) is principal, defined over $\boldsymbol{Q}$. Proposition 1 shows that, in this case, for a prime number l,

case (i) if $(l)=\mathfrak{l}_1\cdot\mathfrak{l}_2$, $\mathfrak{l}_1\neq\mathfrak{l}_2$ in $\boldsymbol{Q}(\sqrt{5})$,

(4.1) $$R_1^{\mathfrak{l}_i}[G(K(\mathfrak{l}_i)/\boldsymbol{Q})]\subset GL(2, \boldsymbol{Z}/(l)),\ i=1,2,$$

and

case (ii) if $(l)=\mathfrak{l}$ remains prime in $\boldsymbol{Q}(\sqrt{5})$,

(4.2) $$R_1^{\mathfrak{l}}\ [G(K(\mathfrak{l})/\boldsymbol{Q})]\subset(\boldsymbol{Z}/(l))^*\cdot SL(2, \mathfrak{o}/\mathfrak{l}),$$

where $\mathfrak{o}$ denotes the ring of integers in $\boldsymbol{Q}(\sqrt{5})$.

Now we can check for several primes $\mathfrak{l}$, the equalities of (4.1) and (4.2) hold. In fact, we can check it by the following steps. Put $S_{\mathfrak{l}}=R_1^{\mathfrak{l}}[G(K(\mathfrak{l})/\boldsymbol{Q})]\cap SL(2, \mathfrak{o}/\mathfrak{l})$. Then, for the equalities of (4.1) and (4.2), it is sufficient to show the followings:

(a) $S_{\mathfrak{l}}=SL(2, \mathfrak{o}/\mathfrak{l})$

and

(b) there exists a prime number p which is a primitive l-th root and satisfies either the property of (A) or (B) in Proposition 2. Moreover, in Dickson [1], all the subgroups of $SL(2, GF(\mathfrak{l}^n))/\{\pm 1\}$ are determined. Hence, by Proposition 2, to check the property (a), we have only to show the next $(a'1) \sim (a'3)$:

$(a'1)$ $S_{\mathfrak{l}} \ni \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$,

$(a'2)$ there exists a prime number p satisfying the propesty (A)

and

$(a'3)$ $S_{\mathfrak{l}}$ contains an element of order $N\mathfrak{l}+1$.

Let us now consider, for example, the case (i) $l=79=\mathfrak{l}_1 \cdot \mathfrak{l}_2$(in $\boldsymbol{Q}(\sqrt{5})$. For $p=31, 47$, we have $c_{31,1}=3\sqrt{5}$, $c_{47,1}=\sqrt{5}$. Hence $p=31$ (resp. $p=47$) satisfies $(a'2)$ (resp. (b)). For $p=19$, we have $c_{19,1}=-2$. By a simple computation, we have $R_1^{\mathfrak{l}_i}(\sigma')^{39}$ ($=X$; say) $\in S_{\mathfrak{l}_i}$, $i=1,2$ and $X^{40}=\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$.Thus we get $G(K(\mathfrak{l}_i)/\boldsymbol{Q}) \cong GL(2, \boldsymbol{Z}/(79))$ for $i=1,2$.

As an example of the case (ii), we choose $l=7$. For $p=3$, we have $c_{3,1}=\sqrt{5}$, for which $(a'2)$ and (b) are satisfied. For $p=11$, we have $c_{11,1}=-3-\sqrt{5}$. We have $R_1^{(7)}(\sigma')^3(=X) \in S_{(7)}$ and $X^{25}=\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$. Thus we get $G(K((7))/\boldsymbol{Q}) \cong (\boldsymbol{Z}/(7))^* \cdot SL(2, GF(7^2))$.

Remark 1. In the above example of case (i), we get $G(K(\mathfrak{l}_1)/\boldsymbol{Q}) \cong G(K(\mathfrak{l}_2)/\boldsymbol{Q})$ $(\cong GL(2, \boldsymbol{Z}/(l)))$. However, in general, this isomorphism can not be hold.

Remark 2. In the case of $\Gamma_0(11)$, it is known, for the elliptic curve J_{11}, $K((5))/\boldsymbol{Q}$ is an abelian extension. Putting $\sqrt[12]{\Delta(z) \cdot \Delta(11z)} = \sum c_n q^n$, $c_p \equiv p+1 \bmod (5)$ for every prime number $p(\neq 11)$. The corresponding fact, in our case, is found in $l=11$. Namely, for $11 = \mathfrak{l}_1 \cdot \mathfrak{l}_2$, $\mathfrak{l}_1=(4+\sqrt{5})$, $\mathfrak{l}_2=(4-\sqrt{5})$, we have $c_{p,1} \equiv p+1 \bmod \mathfrak{l}_1$ for every prime number $p(\neq 23)$.

Remark 3. This was remarked by Prof. G. Shimura. In our discussions of $G(K(\mathfrak{l})/\boldsymbol{Q})$, we restricted ourselves to the case for the prime ideal $\mathfrak{l}$. However, for the integral ideal $\mathfrak{a}$ of F, we have

$$G(K(\mathfrak{a})/\boldsymbol{Q})\subset(\boldsymbol{Z}/(c))^{*}\prod_{\mathfrak{l}|\mathfrak{a}}SL(2,\mathfrak{o}/\mathfrak{l}),$$

where c is the smallest positive integer contained in $\mathfrak{a}$. In particular for a rational prime number l of case (i), we have

$$G(K(l)/\boldsymbol{Q})\subset\{(M,N)\in GL(2,\boldsymbol{Z}/(l))\times GL(2,\boldsymbol{Z}/(l))\mid\det M=\det N\}.$$

Kyoto University

References

[1] L. E. Dickson, Linear groups, Leipzig (1901).
[2] K. Doi, On the jacobian varieties of the fields of elliptic modular functions, Osaka Math. J., 15 (1963), 249–256.
[3] T. Matsui, On the endomorphism algebra of jacobian varieties attached to the field of elliptic modular functions, Osaka J. Math., 1 (1964), 25–31.
[4] G. Shimura and Y. Taniyama, Complex multiplication of abelian varieties and its applications of number theory, Publ. Math. Soc. Japan, No. 6 (1961).
[5] G. Shimura, On the field of definition for a field of automorphic functions II, Ann. of Math., 81 (1965), 124–165.
[6] G. Shimura, A reciprocity law in non-solvable extensions, J. Reine Angew. Math., 221 (1966), 209–220.