Tohoku Math. J.
63 (2011), 413–426

RAY CLASS INVARIANTS OVER IMAGINARY QUADRATIC FIELDS

HO YUN JUNG, JA KYUNG KOO AND DONG HWA SHIN*

(Received August 17, 2010, revised January 27, 2011)

Abstract. Let K be an imaginary quadratic field of discriminant less than or equal to -7 and $K_{(N)}$ be its ray class field modulo N for an integer N greater than 1. We prove that the singular values of certain Siegel functions generate $K_{(N)}$ over K by extending the idea of our previous work. These generators are not only the simplest ones conjectured by Schertz, but also quite useful in the matter of computation of class polynomials. We indeed give an algorithm to find all conjugates of such generators by virtue of the works of Gee and Stevenhagen.

Introduction. Let K be an imaginary quadratic field and $\mathcal{O}_K = \boldsymbol{Z}[\theta]$ be the ring of integers with θ in the complex upper half plane $\mathfrak{H}$. We denote the Hilbert class field and the ray class field modulo N of K for a positive integer N by H and $K_{(N)}$, respectively. Hasse ([8] or [12, Chapter 10, Corollary to Theorem 7]) found in 1927 that for any nonzero integral ideal $\mathfrak{a}$ of K, $K_{(N)}$ is generated over H by adjoining the value of the Weber function for the elliptic curve $\boldsymbol{C}/\mathfrak{a}$ at a generator of the cyclic $\mathcal{O}_K$-module $(1/N)\mathfrak{a}/\mathfrak{a}$. It requires good understanding of the arithmetic of elliptic curves, which is formulated by the theory of complex multiplication ([12, Chapter 10] or [15, Chapter 5]). Together with Shimura's reciprocity law which reveals a remarkable relationship between class field theory and modular function fields, the theory of Shimura's canonical model allows us to generate $K_{(N)}$ over K by the specialization of a certain modular function field. In particular, Cho-Koo [2, Corollary 5.2] showed that the singular value of a Hauptmodul with rational Fourier coefficients on some modular curve generates $K_{(N)}$ over K. For instance, Cho-Koo-Park [3, Theorem 13] considered the case $N = 6$ in terms of Ramanujan's cubic continued fraction. Also Koo-Shin further provided in [10, pp. 161–162] appropriate Hauptmoduli for this purpose.

It seems to be a difficult problem to construct a ray class invariant (as a primitive generator of $K_{(N)}$) over K by means of values of a transcendental function which can be applied to all K and N. In 1964 Ramachandra [13, Theorem 10] at last found universal generators of ray class fields of arbitrary moduli by applying the Kronecker limit formula. However his invariants involve overly complicated products of high powers of singular values of the Klein forms and singular values of the discriminant Δ-function. On the other hand, Schertz [14, Theorems 3 and 4] attempted to find simple and better answers for practical use with similar

2000 *Mathematics Subject Classification.* Primary 11G16; Secondary 11F11, 11F20, 11G15, 11R37.

Key words and phrases. Elliptic units, class field theory, complex multiplication, modular forms.

This research was partially supported by Basic Science Research Program through the NRF of Korea funded by MEST (2011-0001184).

*The corresponding author was partially supported by TJ Park Postdoctoral Fellowship.

ideas. The simplest generators conjectured by Schertz [14, p. 386] are singular values of a Siegel function, and Jung-Koo-Shin [9, Theorem 2.4] showed that his conjectural generators are the right ones at least over H for $K \neq \boldsymbol{Q}(\sqrt{-1}), \boldsymbol{Q}(\sqrt{-3})$.

Since the primitive element theorem guarantees the existence of a simple generator of $K_{(N)}$ over K, one might try to combine Hasse's two generators to get a ray class invariant. Cho-Koo [2, Corollary 5.5] recently succeeded in obtaining such a generator by showing that the singular value of a Weber function is an algebraic integer and then applying the result of Gross-Zagier ([7] or [4, Theorem 13.28]). Koo-Shin [10, Theorems 9.8 and 9.10] further investigated the problem over K in a completely different point of view by using both singular values of the elliptic modular function j and Siegel functions.

For any pair $(r_1, r_2) \in \boldsymbol{Q}^2 \setminus \boldsymbol{Z}^2$ we define the *Siegel function* $g_{(r_1,r_2)}(\tau)$ on $\tau \in \mathfrak{H}$ by the infinite product expansion

$$g_{(r_1,r_2)}(\tau) = -q_\tau^{(1/2)\mathbf{B}_2(r_1)} e^{\pi i r_2(r_1-1)}(1-q_z)\prod_{n=1}^{\infty}(1-q_\tau^n q_z)(1-q_\tau^n q_z^{-1}), \tag{1}$$

where $\mathbf{B}_2(X) = X^2 - X + 1/6$ is the second Bernoulli polynomial, $q_\tau = e^{2\pi i\tau}$ and $q_z = e^{2\pi i z}$ with $z = r_1\tau + r_2$. Then it is a modular unit in the sense of [11, p. 36]. Since its Fourier coefficients are quite small, we are able to estimate and compare the values of the function in order to derive our main theorem.

Let $\mathfrak{a} = [\omega_1, \omega_2]$ be a fractional ideal of K not containing 1, where $\{\omega_1, \omega_2\}$ is an oriented basis such that $\omega_1/\omega_2 \in \mathfrak{H}$. Writing $1 = r_1\omega_1 + r_2\omega_2$ for some $(r_1, r_2) \in \boldsymbol{Q}^2 \setminus \boldsymbol{Z}^2$ we denote

$$g(1, [\omega_1, \omega_2]) = g_{(r_1,r_2)}(\omega_1/\omega_2).$$

When a product of these values becomes a unit, we call it an *elliptic unit*. The 12-th power of the above value depends only on $\mathfrak{a}$ itself [11, Chapter 2, Remark to Theorem 1.2]. So we may write $g^{12}(1, \mathfrak{a})$ instead of $g^{12}(1, [\omega_1, \omega_2])$.

For a nontrivial integral ideal $\mathfrak{f}$ of K, let $I_K(\mathfrak{f})$ be the group of fractional ideals of K which are relatively prime to $\mathfrak{f}$, and $P_{K,1}(\mathfrak{f})$ be the subgroup of $I_K(\mathfrak{f})$ generated by the principal ideals $\alpha\mathcal{O}_K$ for $\alpha \in \mathcal{O}_K$ which satisfies $\alpha \equiv 1 \pmod{\mathfrak{f}}$. Then the ideal class group $I_K(\mathfrak{f})/P_{K,1}(\mathfrak{f})$ is isomorphic to the Galois group of the ray class field $K_\mathfrak{f}$ modulo $\mathfrak{f}$ over K [16, pp. 116–118]. Now we consider the value

$$g^{12N(\mathfrak{f})}(1, \mathfrak{f}),$$

where $N(\mathfrak{f})$ is the smallest positive integer in $\mathfrak{f}$. It belongs to $K_\mathfrak{f}$ [11, Chapter 2, Proposition 1.3 and Chapter 11, Theorem 1.1]. Let $\sigma : I_K(\mathfrak{f})/P_{K,1}(\mathfrak{f}) \to \mathrm{Gal}(K_\mathfrak{f}/K)$ be the Artin map. Then for a ray class $C \in I_K(\mathfrak{f})/P_{K,1}(\mathfrak{f})$, $\sigma(C)$ satisfies the rule

$$g^{12N(\mathfrak{f})}(1, \mathfrak{f})^{\sigma(C)} = g^{12N(\mathfrak{f})}(1, \mathfrak{f}\mathfrak{c}^{-1}), \tag{2}$$

where $\mathfrak{c}$ is a representative integral ideal of C by the theory of complex multiplication [11, pp. 235–236]. In our case we take $\mathfrak{f} = N\mathcal{O}_K$ for an integer N (≥ 2). In this paper, as Schertz

conjectured, we shall show that the singular value

$$g^{12N}(1, N\mathcal{O}_K) = g^{12N}_{(0,1/N)}(\theta)$$

alone, or any one of its integral powers generates $K_{(N)}$ over K ($\neq \boldsymbol{Q}(\sqrt{-1}), \boldsymbol{Q}(\sqrt{-3})$) (Theorem 3.5 and Remark 3.6). While the formula (2) provides all conjugates of $g^{12N}_{(0,1/N)}(\theta)$, it is inconvenient for practical use because we can hardly describe bases of representative ideals in general. Therefore, rather than working with actions of $\mathrm{Gal}(K_{(N)}/K)$ directly by (2) we will manipulate actions of $\mathrm{Gal}(H/K)$ and $\mathrm{Gal}(K_{(N)}/H)$ separately by following Gee-Stevenhagen's idea ([6, §3, 9, 10] or [17, §3, 6]).

1. Fields of modular functions. This section will be devoted to reviewing briefly modular function fields and actions of Galois groups in terms of Siegel functions. For the full description of the modularity of Siegel functions we refer to [10] or [11].

For a positive integer N, let $\zeta_N = e^{2\pi i/N}$ and

$$\Gamma(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\boldsymbol{Z}) \; ; \; \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{N} \right\}$$

be the principal congruence subgroup of level N of $\mathrm{SL}_2(\boldsymbol{Z})$. The group $\Gamma(N)$ acts on $\mathfrak{H}$ by fractional linear transformations, and the orbit space $Y(N) = \Gamma(N)\backslash\mathfrak{H}$ can be given a structure of a Riemann surface. Furthermore, $Y(N)$ can be compactified by adding cusps so that $X(N) = \Gamma(N)\backslash\mathfrak{H}^*$ with $\mathfrak{H}^* = \mathfrak{H} \cup \boldsymbol{P}^1(\boldsymbol{Q})$ becomes a compact Riemann surface (or an algebraic curve), which we call the *modular curve of level N* ([5, Chapter 2] or [15, §1.5]).

Meromorphic functions on $X(N)$ are called *modular functions of level N*. In particular, we are interested in the field of modular functions of level N defined over the N-th cyclotomic field $\boldsymbol{Q}(\zeta_N)$ which is denoted by $\mathcal{F}_N$. Then it is well-known that the extension $\mathcal{F}_N/\mathcal{F}_1$ is Galois and

$$\mathrm{Gal}(\mathcal{F}_N/\mathcal{F}_1) \cong \mathrm{GL}_2(\boldsymbol{Z}/N\boldsymbol{Z})/\{\pm 1_2\}\,,$$

whose action is given as follows: We can decompose an element $\alpha \in \mathrm{GL}_2(\boldsymbol{Z}/N\boldsymbol{Z})/\{\pm 1_2\}$ into $\alpha = \alpha_1 \cdot \alpha_2$ for some $\alpha_1 \in \mathrm{SL}_2(\boldsymbol{Z}/N\boldsymbol{Z})/\{\pm 1_2\}$ and $\alpha_2 = \left(\begin{smallmatrix} 1 & 0 \\ 0 & d \end{smallmatrix}\right)$. The action of α_1 is defined by a fractional linear transformation, and α_2 acts by the rule

$$\sum_{n>-\infty} c_n q_\tau^{n/N} \mapsto \sum_{n>-\infty} c_n^{\sigma_d} q_\tau^{n/N}\,,$$

where $\sum_{n>-\infty} c_n q_\tau^{n/N}$ is the Fourier expansion of a function in $\mathcal{F}_N$ and σ_d is the automorphism of $\boldsymbol{Q}(\zeta_N)$ defined by $\zeta_N^{\sigma_d} = \zeta_N^d$ [12, Chapter 6, Theorem 3].

It is well-known that the fields $\mathcal{F}_N$ are described by $j(\tau)$ and the Fricke functions ([12, Chapter 6, Corollary 1] or [15, Proposition 6.9]). However, we restate these fields in terms of Siegel functions for later use. First, we need some transformation formulas and modularity criterion for Siegel functions. For $X \in \boldsymbol{R}$ we define $\langle X \rangle$ to be the fractional part of X such that $0 \le \langle X \rangle < 1$.

PROPOSITION 1.1. *Let $(r_1, r_2) \in (1/N)\boldsymbol{Z}^2 \setminus \boldsymbol{Z}^2$ for an integer $N \ge 2$.*

(i) $g^{12N}_{(r_1,r_2)}(\tau)$ *satisfies the relation*

$$g^{12N}_{(r_1,r_2)}(\tau) = g^{12N}_{(-r_1,-r_2)}(\tau) = g^{12N}_{(\langle r_1\rangle,\langle r_2\rangle)}(\tau)\,.$$

(ii) $g^{12N}_{(r_1,r_2)}(\tau)$ *belongs to* $\mathcal{F}_N$ *and* $\alpha \in \mathrm{GL}_2(\mathbf{Z}/N\mathbf{Z})/\{\pm 1_2\}$ *acts on it by*

$$g^{12N}_{(r_1,r_2)}(\tau)^\alpha = g^{12N}_{(r_1,r_2)\alpha}(\tau)\,.$$

(iii) $\mathcal{F}_N = \boldsymbol{Q}(\zeta_N)(j(\tau),\ g^{12N}_{(1/N,0)}(\tau),\ g^{12N}_{(0,1/N)}(\tau))$.

PROOF. (i) See [10, Proposition 2.4(1), (3)].

(ii) See [11, Proposition 1.3].

(iii) See [10, Theorem 4.2]. □

We set

$$\mathcal{F} = \bigcup_{N=1}^{\infty} \mathcal{F}_N\,.$$

Passing to the projective limit of exact sequences

$$1 \longrightarrow \{\pm 1_2\} \longrightarrow \mathrm{GL}_2(\mathbf{Z}/N\mathbf{Z}) \longrightarrow \mathrm{Gal}(\mathcal{F}_N/\mathcal{F}_1) \longrightarrow 1$$

for all N (≥ 1), we obtain an exact sequence

$$1 \longrightarrow \{\pm 1_2\} \longrightarrow \prod_{p\,:\,\text{primes}} \mathrm{GL}_2(\mathbf{Z}_p) \longrightarrow \mathrm{Gal}(\mathcal{F}/\mathcal{F}_1) \longrightarrow 1\,. \tag{3}$$

For every $u = (u_p)_p \in \prod_p \mathrm{GL}_2(\mathbf{Z}_p)$ and a positive integer N, there exists an integral matrix α in $\mathrm{GL}_2^+(\boldsymbol{Q})$ with $\det(\alpha) > 0$ such that $\alpha \equiv u_p \pmod{N\mathbf{Z}_p}$ for all p dividing N by the Chinese remainder theorem. The action of u on $\mathcal{F}_N$ can be described by the action of α [15, Proposition 6.21].

2. Shimura's reciprocity law. We shall develop an algorithm for finding all conjugates of the singular value of a modular function, from which we can determine all conjugates of $g^{12N}_{(0,1/N)}(\theta)$. To this end we adopt Gee-Stevenhagen's idea which explains Shimura's reciprocity law explicitly for practical use.

Let $\boldsymbol{A}_{\boldsymbol{Q}}^{\mathrm{f}} = \prod'_p \boldsymbol{Q}_p$ denote the ring of finite adeles. Here, the restricted product is taken with respect to the subrings $\mathbf{Z}_p \subset \boldsymbol{Q}_p$. Every $x \in \mathrm{GL}_2(\boldsymbol{A}_{\boldsymbol{Q}}^{\mathrm{f}})$ can be written as

$$x = u \cdot \alpha \quad \text{with } u \in \prod_p \mathrm{GL}_2(\mathbf{Z}_p) \text{ and } \alpha \in \mathrm{GL}_2^+(\boldsymbol{Q})\,,$$

since the class number of $\boldsymbol{Q}$ is one [15, Lemma 6.19]. Such a decomposition $x = u \cdot \alpha$ determines a group action of $\mathrm{GL}_2(\boldsymbol{A}_{\boldsymbol{Q}}^{\mathrm{f}})$ on $\mathcal{F}$ by

$$h^x = h^u \circ \alpha\,,$$

where h^u is given by the exact sequence (3) [15, pp. 149–150]. Then we have *Shimura's exact sequence*

$$1 \longrightarrow \boldsymbol{Q}^* \longrightarrow \mathrm{GL}_2(\boldsymbol{A}_{\boldsymbol{Q}}^{\mathrm{f}}) \longrightarrow \mathrm{Aut}(\mathcal{F}) \longrightarrow 1$$

[15, Theorem 6.23].

Let K be an imaginary quadratic field of discriminant d_K. From now on we fix

$$\theta = \begin{cases} \sqrt{d_K}/2 & \text{for } d_K \equiv 0 \pmod 4, \\ (-1+\sqrt{d_K})/2 & \text{for } d_K \equiv 1 \pmod 4, \end{cases} \tag{4}$$

which satisfies $\mathcal{O}_K = \boldsymbol{Z}[\theta]$. Then its minimal polynomial over $\boldsymbol{Q}$ is

$$X^2 + B_\theta X + C_\theta = \begin{cases} X^2 - d_K/4 & \text{if } d_K \equiv 0 \pmod 4, \\ X^2 + X + (1-d_K)/4 & \text{if } d_K \equiv 1 \pmod 4. \end{cases}$$

We use the notation $K_p = K \otimes_{\boldsymbol{Q}} \boldsymbol{Q}_p$ for each prime p and denote the group of finite ideles of K by $(\boldsymbol{A}_K^{\mathrm{f}})^* = \prod_p' K_p^*$, where the restricted product is taken with respect to the subgroups $\mathcal{O}_p^* = (\mathcal{O}_K \otimes_{\boldsymbol{Z}} \boldsymbol{Z}_p)^*$ of K_p^*. Let $[\cdot, K]$ denote the Artin map on $(\boldsymbol{A}_K^{\mathrm{f}})^*$. Then the class field theory on K is summarized in the exact sequence

$$1 \longrightarrow K^* \longrightarrow (\boldsymbol{A}_K^{\mathrm{f}})^* \xrightarrow{[\cdot,K]} \mathrm{Gal}(K^{\mathrm{ab}}/K) \longrightarrow 1,$$

where K^{ab} is the maximal abelian extension of K ([15, §5.2] or [16, Chapter II, Theorem 3.5]). The main theorem of the theory of complex multiplication states that the value $j(\theta)$ generates H over K, and the sequence

$$1 \longrightarrow \mathcal{O}_K^* \longrightarrow \prod_p \mathcal{O}_p^* \xrightarrow{[\cdot,K]} \mathrm{Gal}(K^{\mathrm{ab}}/K(j(\theta))) \longrightarrow 1 \tag{5}$$

is exact [15, Theorem 5.7]. Furthermore, $K_{(N)}$ is none other than the field $K(\mathcal{F}_N(\theta))$ which is the extension field of K obtained by adjoining all singular values $h(\theta)$ for $h \in \mathcal{F}_N$ which is defined and finite at θ ([12, Chapter 10, Corollary to Theorem 2] or [15, Proposition 6.33]).

For each prime p we define

$$(g_\theta)_p : K_p^* \longrightarrow \mathrm{GL}_2(\boldsymbol{Q}_p)$$

as the injection that sends $x_p \in K_p^*$ to the matrix in $\mathrm{GL}_2(\boldsymbol{Q}_p)$ which represents the multiplication by x_p with respect to the $\boldsymbol{Q}_p$-basis $\binom{\theta}{1}$ for K_p. More precisely, if $\min(\theta, \boldsymbol{Q}) = X^2 + B_\theta X + C_\theta$, then for $s_p,\ t_p \in \boldsymbol{Q}_p$ we can describe the map as

$$(g_\theta)_p \ :\ s_p\theta + t_p \mapsto \begin{pmatrix} t_p - B_\theta s_p & -C_\theta s_p \\ s_p & t_p \end{pmatrix}.$$

On $(\boldsymbol{A}_K^{\mathrm{f}})^*$ we have an injection

$$g_\theta = \prod_p (g_\theta)_p \ :\ (\boldsymbol{A}_K^{\mathrm{f}})^* \longrightarrow \prod_p{}' \mathrm{GL}_2(\boldsymbol{Q}_p),$$

where the restricted product is taken with respect to the subgroups $\mathrm{GL}_2(\boldsymbol{Z}_p)$ of $\mathrm{GL}_2(\boldsymbol{Q}_p)$. Combining (3) and (5) we get the diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathcal{O}^* & \longrightarrow & \prod_p \mathcal{O}_p^* & \xrightarrow{[\cdot,K]} & \mathrm{Gal}(K^{\mathrm{ab}}/K(j(\theta))) & \longrightarrow & 1 \\ & & & & \downarrow g_\theta & & & & \\ 1 & \longrightarrow & \{\pm 1_2\} & \longrightarrow & \prod_p \mathrm{GL}_2(\boldsymbol{Z}_p) & \longrightarrow & \mathrm{Gal}(\mathcal{F}/\mathcal{F}_1) & \longrightarrow & 1. \end{array} \tag{6}$$

Then *Shimura's reciprocity law* says that for $h \in \mathcal{F}$ and $x \in \prod_p \mathcal{O}_p^*$

$$h(\theta)^{[x^{-1},K]} = h^{(g_\theta(x))}(\theta) \tag{7}$$

[15, Theorem 6.31].

Let $Q = [a, b, c] = aX^2 + bXY + cY^2 \in \boldsymbol{Z}[X, Y]$ be a primitive positive definite quadratic form of discriminant d_K. Under an appropriate equivalence relation these forms determine the group $\mathrm{C}(d_K)$, called the *form class group of discriminant* d_K. In particular, the unit element is the class containing

$$\begin{cases} [1, 0, -d_K/4] & \text{for } d_K \equiv 0 \pmod 4, \\ [1, 1, (1-d_K)/4] & \text{for } d_K \equiv 1 \pmod 4, \end{cases} \tag{8}$$

and the inverse of the class containing $[a, b, c]$ is the class containing $[a, -b, c]$ [4, Theorem 3.9]. We identify $\mathrm{C}(d_K)$ with the set of all *reduced quadratic forms*, which are characterized by the conditions

$$(-a < b \le a < c \quad \text{or} \quad 0 \le b \le a = c) \quad \text{and} \quad b^2 - 4ac = d_K \tag{9}$$

[4, Theorem 2.8]. Note that the above two conditions for reduced quadratic forms imply

$$a \le \sqrt{-d_K/3} \tag{10}$$

[4, p. 29]. It is well-known that $\mathrm{C}(d_K)$ is isomorphic to $\mathrm{Gal}(H/K)$ [4, Theorem 7.7]. Gee and Stevenhagen found an idele $x_Q \in (\boldsymbol{A}_K^{\mathrm{f}})^*$ such that

$$[x_Q, K]|_H = [a, b, c].$$

PROPOSITION 2.1. *Let $Q = [a, b, c]$ be a primitive positive definite quadratic form of discriminant d_K. We put*

$$\theta_Q = (-b + \sqrt{d_K})/2a.$$

Furthermore, for each prime p we define x_p as

$$x_p = \begin{cases} a & \text{if } p \nmid a, \\ a\theta_Q & \text{if } p \mid a \text{ and } p \nmid c, \\ a(\theta_Q - 1) & \text{if } p \mid a \text{ and } p \mid c. \end{cases}$$

Then for $x_Q = (x_p)_p \in (\boldsymbol{A}_K^{\mathrm{f}})^*$ the Galois action of the Artin symbol $[x_Q, K]$ satisfies the relation

$$j(\theta)^{[a,b,c]} = j(\theta)^{[x_Q,K]}.$$

PROOF. See [6, Lemma 19] or [17, §6]. □

The next proposition gives the action of $[x_Q^{-1}, K]$ on K^{ab} by using Shimura's reciprocity law (7).

PROPOSITION 2.2. *Let $Q = [a, b, c]$ be a primitive positive definite quadratic form of discriminant d_K and θ_Q be as in Proposition* 2.1. *Define $u_Q = (u_p)_p \in \prod_p \mathrm{GL}_2(\boldsymbol{Z}_p)$ as*

Case 1 : $d_K \equiv 0 \pmod 4$

$$u_p = \begin{cases} \begin{pmatrix} a & b/2 \\ 0 & 1 \end{pmatrix} & \text{if } p \nmid a\,, \\ \begin{pmatrix} -b/2 & -c \\ 1 & 0 \end{pmatrix} & \text{if } p \mid a \text{ and } p \nmid c\,, \\ \begin{pmatrix} -a-b/2 & -c-b/2 \\ 1 & -1 \end{pmatrix} & \text{if } p \mid a \text{ and } p \mid c\,, \end{cases} \tag{11}$$

Case 2 : $d_K \equiv 1 \pmod 4$

$$u_p = \begin{cases} \begin{pmatrix} a & (b-1)/2 \\ 0 & 1 \end{pmatrix} & \text{if } p \nmid a\,, \\ \begin{pmatrix} -(b+1)/2 & -c \\ 1 & 0 \end{pmatrix} & \text{if } p \mid a \text{ and } p \nmid c\,, \\ \begin{pmatrix} -a-(b+1)/2 & -c+(1-b)/2 \\ 1 & -1 \end{pmatrix} & \text{if } p \mid a \text{ and } p \mid c\,. \end{cases} \tag{12}$$

Then for $h \in \mathcal{F}$ which is defined and finite at θ we have

$$h(\theta)^{[x_Q^{-1},K]} = h^{u_Q}(\theta_Q)\,.$$

PROOF. See [6, Lemma 20] or [17, §6]. □

For each positive integer N we put

$$W_{N,\theta} = \left\{ \begin{pmatrix} t - B_\theta s & -C_\theta s \\ s & t \end{pmatrix} \in \mathrm{GL}_2(\mathbf{Z}/N\mathbf{Z})\ ;\ t,\ s \in \mathbf{Z}/N\mathbf{Z} \right\}.$$

Analyzing the diagram (6) and using Shimura's reciprocity law (7), Gee and Stevenhagen could express $\mathrm{Gal}(K_{(N)}/H)$ quite explicitly.

PROPOSITION 2.3. *Assume that $K \neq \boldsymbol{Q}(\sqrt{-1}), \boldsymbol{Q}(\sqrt{-3})$ and $N \geq 1$. Then we have a surjective homomorphism*

$$\begin{array}{ccc} W_{N,\theta} & \longrightarrow & \mathrm{Gal}(K_{(N)}/H) \\ \cup & & \cup \\ \alpha & \longmapsto & (h(\theta) \mapsto h^\alpha(\theta))_{h \in \mathcal{F}_{N,\theta}}, \end{array}$$

where $\mathcal{F}_{N,\theta} = \{h \in \mathcal{F}_N\ ;\ h \text{ is defined and finite at } \theta\}$. The kernel of this homomorphism is $\{\pm 1_2\}$ by (6) *and* (7).

PROOF. See [6, pp. 50–51] or [17, §3]. □

Finally we obtain an assertion which we shall use to solve our main problem. In the next theorem, we follow the notations in Propositions 2.2 and 2.3.

THEOREM 2.4. *Assume that $K \neq \boldsymbol{Q}(\sqrt{-1}), \boldsymbol{Q}(\sqrt{-3})$ and $N \geq 1$. Then there is a one-to-one correspondence*

$$\begin{array}{ccc} W_{N,\theta}/\{\pm 1_2\} \times \mathrm{C}(d_K) & \longrightarrow & \mathrm{Gal}(K_{(N)}/K) \\ \cup & & \cup \\ (\alpha,\, Q) & \longmapsto & (h(\theta) \mapsto h^{\alpha \cdot u_Q}(\theta_Q))_{h \in \mathcal{F}_{N,\theta}} . \end{array}$$

Here, we follow notations in Propositions 2.2 *and* 2.3.

PROOF. Observe the following diagram:

$$\begin{array}{ll} \underline{\text{Fields}} & \underline{\text{Galois groups}} \\ K_{(N)} & \\ \Big| \Big) & \mathrm{Gal}(K_{(N)}/H) \simeq W_{N,\theta}/\{\pm 1_2\} \quad \text{by Proposition 2.3} \\ H & \\ \Big| \Big) & \mathrm{Gal}(H/K) = \{[x_Q, K]|_H \,;\; Q \in \mathrm{C}(d_K)\} \quad \text{by Proposition 2.1.} \\ K & \end{array}$$

Now the conclusion follows from Proposition 2.2. □

REMARK 2.5. In particular, the unit element of $W_{N,\theta}/\{\pm 1_2\} \times \mathrm{C}(d_K)$ corresponds to the unit element of $\mathrm{Gal}(K_{(N)}/K)$ by the definitions of u_Q and θ_Q. Note that the correspondence is not a group homomorphism.

3. Ray class invariants. In this last section we shall prove that the singular value $g^{12N}_{(0,1/N)}(\theta)$ generates $K_{(N)}$ by showing that the only automorphism of $K_{(N)}$ over K which fixes it is the unit element. Then Galois theory guarantees our theorem. Although we leave out finitely many cases, one can readily verify that the remaining cases are indeed generators of $K_{(N)}$ over K by computing minimal polynomials of the singular values if desired.

Throughout this section we let K ($\neq \boldsymbol{Q}(\sqrt{-1}), \boldsymbol{Q}(\sqrt{-3})$) be an imaginary quadratic field of discriminant d_K such that $d_K \leq -7$. We put $D = \sqrt{-d_K/3}$ and define θ, θ_Q, u_Q for each primitive positive definite quadratic form $Q = [a, b, c]$ as in (4) and Proposition 2.2. If we set

$$B = |q_\theta| = |e^{2\pi i \theta}| = e^{-\pi\sqrt{-d_K}} ,$$

then we have

$$B \leq e^{-\sqrt{7}\pi} \quad \text{and} \quad B^{1/D} = e^{-\sqrt{3}\pi} . \tag{13}$$

In what follows we shall often use the basic inequality

$$1 + X < e^X \quad \text{for } X > 0 . \tag{14}$$

LEMMA 3.1. *We have the following inequalities*:

(i) *If* $N \geq 21$, *then* $|(1-\zeta_N)/(1-B^{1/DN})| < 1.306$.
(ii) *If* $N \geq 2$, *then* $|(1-\zeta_N)/(1-\zeta_N^s)| \leq 1$ *for all* $s \in \boldsymbol{Z} \setminus N\boldsymbol{Z}$.
(iii) *If* $N \geq 4$, *then* $|(1-\zeta_N)/(1-\zeta_N^s)| \leq 1/\sqrt{2}$ *for* $2 \leq s \leq N/2$.
(iv) *If* $N \geq 2$, *then* $B^{(1/2)(\mathbf{B}_2(0)-\mathbf{B}_2(1/N))}|(1-\zeta_N)/(1-B^{1/N})| < 0.76$.

(v) $1/(1-B^{X/D}) < 1+B^{X/1.03D}$ *for all* $X \geq 1/2$.

(vi) $1/(1-B^{X}) < 1+B^{X/1.03}$ *for all* $X \geq 1/2$.

PROOF. (i) It is routine to check that $|(1-\zeta_N)/(1-B^{1/DN})| = 2\sin(\pi/N)/(1-e^{-\sqrt{3}\pi/N})$ is a decreasing function for $N \geq 21$. Hence its value is maximal when $N = 21$, which is less than 1.306.

(ii) $|(1-\zeta_N)/(1-\zeta_N^s)| = |\sin(\pi/N)/\sin(\pi s/N)| \leq 1$ for all $s \in \mathbf{Z} \setminus N\mathbf{Z}$.

(iii) If $N \geq 4$ and $2 \leq s \leq N/2$, then $|\sin(s\pi/N)| \geq \sin(2\pi/N)$. Thus

$$\left|\frac{1-\zeta_N}{1-\zeta_N^s}\right| = \left|\frac{\sin(\pi/N)}{\sin(s\pi/N)}\right| \leq \frac{\sin(\pi/N)}{\sin(2\pi/N)} = \frac{1}{2\cos(\pi/N)} \leq \frac{1}{2\cos(\pi/4)} = \frac{1}{\sqrt{2}}.$$

(iv) Observe that

$$B^{(1/2)(\mathbf{B}_2(0)-\mathbf{B}_2(1/N))}\left|\frac{1-\zeta_N}{1-B^{1/N}}\right| \leq e^{(-\sqrt{7}\pi/2)(1/N-1/N^2)}\frac{2\sin(\pi/N)}{1-e^{-\sqrt{7}\pi/N}} \quad \text{(by (13))}.$$

It is also routine to check the last term on N (≥ 2) is less than 0.76.

(v) By (13) the inequality is equivalent to $e^{-\sqrt{3}\pi X} + e^{-3\sqrt{3}\pi X/103} < 1$, which obviously holds for $X \geq 1/2$.

(vi) The given inequality is equivalent to $B^X + B^{3X/103} < 1$. By (13) it suffices to show $e^{-\sqrt{7}\pi X} + e^{-3\sqrt{7}\pi X/103} < 1$, which is true for all $X \geq 1/2$. □

LEMMA 3.2. *Let* $N \geq 21$ *and* $Q = [a, b, c]$ *be a reduced quadratic form of discriminant* d_K. *If* $a \geq 2$, *then the inequality*

$$|g_{(0,1/N)}(\theta)| < |g_{(r/N,s/N)}(\theta_Q)|$$

holds for $(r, s) \in \mathbf{Z}^2 \setminus N\mathbf{Z}^2$.

PROOF. We may assume $0 \leq r \leq N/2$ by Proposition 1.1(i). Also note that $2 \leq a \leq D$ by (10). From (1) we obtain that

$$\begin{aligned}\left|\frac{g_{(0,1/N)}(\theta)}{g_{(r/N,s/N)}(\theta_Q)}\right| &= \left|\frac{g_{(0,1/N)}(\theta)}{g_{(r/N,s/N)}((-b+\sqrt{d_K})/2a)}\right| \\ &\leq B^{(1/2)(\mathbf{B}_2(0)-(1/a)\mathbf{B}_2(r/N))}\left|\frac{1-\zeta_N}{1-e^{2\pi i((r/N)(-b+\sqrt{d_K})/2a+s/N)}}\right| \\ &\quad \times \prod_{n=1}^{\infty}\frac{(1+B^n)^2}{(1-B^{(1/a)(n+r/N)})(1-B^{(1/a)(n-r/N)})}.\end{aligned}$$

If $r \neq 0$, then by the fact $2 \leq a \leq D$ and Lemma 3.1(i),

$$\left|\frac{1-\zeta_N}{1-e^{2\pi i((r/N)(-b+\sqrt{d_K})/2a+s/N)}}\right| \leq \left|\frac{1-\zeta_N}{1-B^{r/Na}}\right| \leq \left|\frac{1-\zeta_N}{1-B^{1/ND}}\right| < 1.306.$$

If $r = 0$, then by Lemma 3.1(ii),

$$\left|\frac{1-\zeta_N}{1-e^{2\pi i((r/N)(-b+\sqrt{d_K})/2a+s/N)}}\right| = \left|\frac{1-\zeta_N}{1-\zeta_N^s}\right| \leq 1.$$

Therefore,

$$\begin{aligned}
&\left|\frac{g_{(0,1/N)}(\theta)}{g_{(r/N,s/N)}(\theta_Q)}\right| \\
&< B^{(1/2)(\mathbf{B}_2(0)-(1/2)\mathbf{B}_2(0))}\cdot 1.306\cdot\prod_{n=1}^{\infty}\frac{(1+B^n)^2}{(1-B^{n/D})(1-B^{(1/D)(n-1/2)})} \\
&\quad (\text{since } 2\le a\le D,\ 0\le r\le N/2) \\
&< 1.306B^{1/24}\prod_{n=1}^{\infty}(1+B^n)^2(1+B^{n/1.03D})(1+B^{(1/1.03D)(n-1/2)}) \quad (\text{by Lemma 3.1(v)}) \\
&< 1.306B^{1/24}\prod_{n=1}^{\infty}e^{2B^n+B^{n/1.03D}+B^{(1/1.03D)(n-1/2)}} \quad (\text{by (14)}) \\
&= 1.306B^{1/24}e^{2B/(1-B)+(B^{1/1.03D}+B^{1/2.06D})/(1-B^{1/1.03D})} \\
&\le 1.306e^{-\sqrt{7}\pi/24}e^{2e^{-\sqrt{7}\pi}/(1-e^{-\sqrt{7}\pi})+(e^{-\sqrt{3}\pi/1.03}+e^{-\sqrt{3}\pi/2.06})/(1-e^{-\sqrt{3}\pi/1.03})}<1 \quad (\text{by (13)}).
\end{aligned}$$

This proves the lemma. □

LEMMA 3.3. *Let $N\ge 2$ and $Q=[1,b,c]$ be a reduced quadratic form of discriminant d_K. Then we have the inequality*

$$|g_{(0,1/N)}(\theta)|<|g_{(r/N,s/N)}(\theta_Q)|$$

for $r,\ s\in\mathbf{Z}$ with $r\not\equiv 0 \pmod N$.

PROOF. We may assume $1\le r\le N/2$ by Proposition 1.1(i). Then

$$\begin{aligned}
&\left|\frac{g_{(0,1/N)}(\theta)}{g_{(r/N,s/N)}(\theta_Q)}\right| \\
&\le B^{(1/2)(\mathbf{B}_2(0)-\mathbf{B}_2(r/N))}\left|\frac{1-\zeta_N}{1-B^{r/N}}\right|\prod_{n=1}^{\infty}\frac{(1+B^n)^2}{(1-B^{n+r/N})(1-B^{n-r/N})} \quad (\text{by (1)}) \\
&< B^{(1/2)(\mathbf{B}_2(0)-\mathbf{B}_2(1/N))}\left|\frac{1-\zeta_N}{1-B^{1/N}}\right|\prod_{n=1}^{\infty}\frac{(1+B^n)^2}{(1-B^n)(1-B^{n-1/2})} \\
&< 0.76\prod_{n=1}^{\infty}(1+B^n)^2(1+B^{n/1.03})(1+B^{(1/1.03)(n-1/2)}) \quad (\text{by Lemma 3.1(iv) and (vi)}) \\
&< 0.76\prod_{n=1}^{\infty}e^{2B^n+B^{n/1.03}+B^{(1/1.03)(n-1/2)}} \quad (\text{by (14)}) \\
&= 0.76e^{2B/(1-B)+(B^{1/1.03}+B^{1/2.06})/(1-B^{1/1.03})} \\
&\le 0.76e^{2e^{-\sqrt{7}\pi}/(1-e^{-\sqrt{7}\pi})+(e^{-\sqrt{7}\pi/1.03}+e^{-\sqrt{7}\pi/2.06})/(1-e^{-\sqrt{7}\pi/1.03})}<1 \quad (\text{by (13)}).
\end{aligned}$$

□

LEMMA 3.4. *Let $N \geq 2$ and $Q = [1, b, c]$ be a reduced quadratic form of discriminant d_K. Then*

$$|g_{(0,1/N)}(\theta)| < |g_{(0,s/N)}(\theta_Q)|$$

for $s \in \boldsymbol{Z}$ with $s \not\equiv 0, \pm 1 \pmod N$.

PROOF. If $N = 2$ or 3, there is nothing to prove. Thus, let $N \geq 4$. Here we may assume that $2 \leq s \leq N/2$ by Proposition 1.1(i). Observe that

$$\begin{aligned}
&\left| \frac{g_{(0,1/N)}(\theta)}{g_{(0,s/N)}(\theta_Q)} \right| \\
&\leq \left| \frac{1-\zeta_N}{1-\zeta_N^s} \right| \prod_{n=1}^{\infty} \frac{(1+B^n)^2}{(1-B^n)^2} \quad \text{(by (1))} \\
&< (1/\sqrt{2}) \prod_{n=1}^{\infty} (1+B^n)^2 (1+B^{n/1.03})^2 \quad \text{(by Lemma 3.1(iii) and (vi))} \\
&< (1/\sqrt{2}) \prod_{n=1}^{\infty} e^{2B^n + 2B^{n/1.03}} \quad \text{(by (14))} \\
&= (1/\sqrt{2}) e^{2B/(1-B) + 2B^{1/1.03}/(1-B^{1/1.03})} \\
&\leq (1/\sqrt{2}) e^{2e^{-\sqrt{7}\pi}/(1-e^{-\sqrt{7}\pi}) + 2e^{-\sqrt{7}\pi/1.03}/(1-e^{-\sqrt{7}\pi/1.03})} < 1 \quad \text{(by (13))},
\end{aligned}$$

which proves the lemma. □

Now we are ready to prove our main theorem.

THEOREM 3.5. *Let $N \geq 21$. Let K ($\neq \boldsymbol{Q}(\sqrt{-1}), \boldsymbol{Q}(\sqrt{-3})$) be an imaginary quadratic field and θ be as in* (4)*. Then for any positive integer n the value*

$$g^{12Nn}(1, N\mathcal{O}_K) = g_{(0,1/N)}^{12Nn}(\theta)$$

generates $K_{(N)}$ over K. It is a real algebraic integer and its minimal polynomial has integer coefficients. In particular, if N has at least two prime factors, then it is an elliptic unit.

PROOF. For simplicity we put $g(\tau) = g_{(0,1/N)}^{12Nn}(\tau)$. Since g belongs to $\mathcal{F}_N$ by Proposition 1.1(ii), the value $g(\theta)$ lies in $K_{(N)}$ by the main theorem of the theory of complex multiplication. Hence, if we show that the only element of $\mathrm{Gal}(K_{(N)}/K)$ fixing the value $g(\theta)$ is the unit element, then we can conclude that it generates $K_{(N)}$ over K by Galois theory.

By Theorem 2.4 any conjugate of $g(\theta)$ is of the form $g^{\alpha \cdot u_Q}(\theta_Q)$ for some $\alpha = \left(\begin{smallmatrix} t - B_\theta s & -C_\theta s \\ s & t \end{smallmatrix}\right) \in W_{N,\theta}$ and a reduced quadratic form $Q = [a, b, c]$ of discriminant d_K. Assume that $g(\theta) = g^{\alpha \cdot u_Q}(\theta_Q)$. Then Lemma 3.2 implies that $a = 1$, which yields

$$u_Q = \begin{cases} \begin{pmatrix} 1 & b/2 \\ 0 & 1 \end{pmatrix} & \text{for } d_K \equiv 0 \pmod 4, \\ \begin{pmatrix} 1 & (b-1)/2 \\ 0 & 1 \end{pmatrix} & \text{for } d_K \equiv 1 \pmod 4 \end{cases}$$

as an element of $\mathrm{GL}_2(\boldsymbol{Z}/N\boldsymbol{Z})$ by (11) and (12). It follows from Proposition 1.1(ii) that

$$g(\theta) = g^{\alpha \cdot u_Q}(\theta_Q) = g^{12Nn}_{(0,1/N)\alpha u_Q}(\theta_Q) = \begin{cases} g^{12Nn}_{(s/N,(s/N)(b/2)+t/N)}(\theta_Q) & \text{for } d_K \equiv 0 \pmod 4, \\ g^{12Nn}_{(s/N,(s/N)(b-1)/2+t/N)}(\theta_Q) & \text{for } d_K \equiv 1 \pmod 4, \end{cases}$$

from which we get $s \equiv 0 \pmod N$ by Lemma 3.3. Now Lemma 3.4 implies that $t \equiv \pm 1 \pmod N$, which shows that α is the unit element of $W_{N,\theta}/\{\pm 1_2\}$. Finally (9) implies that

$$Q = [a, b, c] = \begin{cases} [1, 0, -d_K/4] & \text{for } d_K \equiv 0 \pmod 4, \\ [1, 1, (1-d_K)/4] & \text{for } d_K \equiv 1 \pmod 4, \end{cases}$$

which represents the unit element of $\mathrm{C}(d_K)$ by (8). This implies that $(\alpha, Q) \in W_{N,\theta}/\{\pm 1_2\} \times \mathrm{C}(d_K)$ represents the unit element of $\mathrm{Gal}(K_{(N)}/K)$ by Remark 2.5. Therefore $g(\theta)$ actually generates $K_{(N)}$ over K.

From (1) we have

$$\begin{aligned} g(\theta) &= \left(q_\theta^{1/12}(1-\zeta_N) \prod_{n=1}^{\infty} (1-q_\theta^n \zeta_N)(1-q_\theta^n \zeta_N^{-1}) \right)^{12Nn} \\ &= q_\theta^{Nn} (2\sin(\pi/N))^{12Nn} \prod_{n=1}^{\infty} (1-(\zeta_N+\zeta_N^{-1})q_\theta^n + q_\theta^{2n})^{12Nn}, \end{aligned}$$

and this shows that $g(\theta)$ is a real number. Furthermore, we see from [10, §3] that the function $g(\tau)$ is integral over $\boldsymbol{Z}[j(\tau)]$. Since $j(\theta)$ is a real algebraic integer [12, Chapter 5, Theorem 4], so is the value $g(\theta)$, and its minimal polynomial over K has integer coefficients. In particular, if N has at least two prime factors, the function $1/g(\tau)$ is also integral over $\boldsymbol{Z}[j(\tau)]$ [11, Chapter 2, Theorem 2.2]; hence $g(\theta)$ becomes a unit. □

REMARK 3.6. (i) If we assume that

$$(15) \qquad (N = 2,\ d_K \le -43) \quad \text{or} \quad (N = 3,\ d_K \le -39) \quad \text{or} \quad (N \ge 4,\ d_K \le -31),$$

then the upper bounds of the inequalities appeared in Lemma 3.1 should be slightly changed. But it is routine to check that Lemmas 3.2 through 3.4 are also true. Therefore we can establish Theorem 3.5 again under the condition (15), however, we shall not repeat the similar proofs.

(ii) Theorem 3.5 is still valid for all $N \ge 2$ and $K \ne \boldsymbol{Q}(\sqrt{-1}), \boldsymbol{Q}(\sqrt{-3})$. Indeed, for the remaining finite cases ($N = 2,\ -40 \le d_K \le -7$), ($N = 3,\ -35 \le d_K \le -7$), ($4 \le N \le 20,\ -24 \le d_K \le -7$) one can readily verify Lemmas 3.2 through 3.4 by Theorem 2.4 and some numerical estimate, not by using Lemma 3.1.

REMARK 3.7. (i) For $N \ge 2$ and $(r_1, r_2) \in (1/N)\boldsymbol{Z}^2 \backslash \boldsymbol{Z}^2$, the function $g^{12N/\gcd(6,N)}_{(r_1,r_2)}(\tau)$ belongs to $\mathcal{F}_N$ and satisfies the same transformation formulas as in Proposition 1.1(i) and (ii) by [10, Theorem 2.5 and Proposition 2.4]. Hence we are able to replace the value $g^{12Nn}_{(0,1/N)}(\theta)$ in Theorem 3.5 by $g^{12Nn/\gcd(6,N)}_{(0,1/N)}(\theta)$ with smaller exponent, which enables us to have class polynomials with relatively small coefficients.

(ii) Nevertheless, the exponent of $g_{(0,1/N)}^{12N/\gcd(6,N)}(\theta)$ could be quite high for numerical computations. So one usually takes suitable products of Siegel functions with lower exponents [1].

(iii) In order to prove that the singular value $g_{(0,1/N)}^{12N/\gcd(6,N)}(\theta)$ is a unit, it suffices to check whether N has more than one prime ideal factor in K [13, §6].

Now we close this section by presenting an example which illustrates Theorem 3.5, Remarks 3.6 and 3.7.

EXAMPLE 3.8. Let $K = \boldsymbol{Q}(\sqrt{-10})$ and $N = 6\ (= 2 \cdot 3)$. Then $d_K = -40$ and $\theta = \sqrt{-10}$. The reduced quadratic forms of discriminant d_K are

$$Q_1 = [1,\ 0,\ 10] \quad \text{and} \quad Q_2 = [2,\ 0,\ 5]\,.$$

So we have

$$\theta_{Q_1} = \sqrt{-10},\ u_{Q_1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad \theta_{Q_2} = \sqrt{-10}/2,\ u_{Q_2} = \begin{pmatrix} 2 & -3 \\ 3 & 4 \end{pmatrix}.$$

Furthermore, one can compute the group $W_{6,\theta}/\{\pm 1_2\}$ easily and the result is as follows:

$$W_{6,\theta}/\{\pm 1_2\} = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 4 \\ 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 4 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 4 \\ 5 & 1 \end{pmatrix}, \begin{pmatrix} 3 & 2 \\ 1 & 3 \end{pmatrix}, \begin{pmatrix} 3 & 4 \\ 2 & 3 \end{pmatrix} \right\}.$$

Thus the class polynomial is

$$\begin{aligned}
\min(g_{(0,1/6)}^{12}(\theta), K) &= \prod_{r=1}^{2} \prod_{\alpha \in W_{6,\theta}/\{\pm 1_2\}} (X - g_{(0,1/6)\alpha u_{Q_r}}^{12}(\theta_{Q_r})) \\
&= (X - g_{(0,1/6)}^{12}(\sqrt{-10}))(X - g_{(1/6,1/6)}^{12}(\sqrt{-10}))(X - g_{(2/6,1/6)}^{12}(\sqrt{-10})) \\
&\quad (X - g_{(3/6,1/6)}^{12}(\sqrt{-10}))(X - g_{(4/6,1/6)}^{12}(\sqrt{-10}))(X - g_{(5/6,1/6)}^{12}(\sqrt{-10})) \\
&\quad (X - g_{(1/6,3/6)}^{12}(\sqrt{-10}))(X - g_{(2/6,3/6)}^{12}(\sqrt{-10}))(X - g_{(3/6,4/6)}^{12}(\sqrt{-10}/2)) \\
&\quad (X - g_{(5/6,1/6)}^{12}(\sqrt{-10}/2))(X - g_{(1/6,4/6)}^{12}(\sqrt{-10}/2))(X - g_{(3/6,1/6)}^{12}(\sqrt{-10}/2)) \\
&\quad (X - g_{(5/6,4/6)}^{12}(\sqrt{-10}/2))(X - g_{(1/6,1/6)}^{12}(\sqrt{-10}/2))(X - g_{(5/6,3/6)}^{12}(\sqrt{-10}/2)) \\
&\quad (X - g_{(1/6,0)}^{12}(\sqrt{-10}/2)) \\
&= X^{16} + 20560X^{15} - 1252488X^{14} - 829016560X^{13} - 8751987701092X^{12} \\
&\quad + 217535583987600X^{11} + 181262520621110344X^{10} + 43806873084101200X^{9} \\
&\quad - 278616280004972730X^{8} + 139245187265282800X^{7} - 8883048242697656X^{6} \\
&\quad + 352945014869040X^{5} + 23618989732508X^{4} - 1848032773840X^{3} \\
&\quad + 49965941112X^{2} - 425670800X + 1\,,
\end{aligned}$$

which shows that $g_{(0,1/6)}^{12}(\theta)$ is also a unit.

REFERENCES

[1] S. BETTNER AND R. SCHERTZ, Lower powers of elliptic units, J. Théor. Nombres Bordeaux 13 (2001), 339–351.
[2] B. CHO AND J. K. KOO, Constructions of class fields over imaginary quadratic fields and applications, Q. J. Math. 61 (2010), 199–216.
[3] B. CHO, J. K. KOO AND Y. K. PARK, On Ramanujan's cubic continued fraction as modular function, Tohoku Math. J. 62 (2010), 579–603.
[4] D. A. COX, Primes of the form $x^2 + ny^2$, Fermat, class field, and complex multiplication, John Wiley & Sons, Inc., New York, 1989.
[5] F. DIAMOND AND J. SHURMAN, A first course in modular forms, Grad. Texts in Math. 228, Springer, New York, 2005.
[6] A. GEE, Class invariants by Shimura's reciprocity law, J. Théor. Nombres Bordeaux 11 (1999), 45–72.
[7] B. GROSS AND D. ZAGIER, On singular moduli, J. Reine Angew. Math. 355 (1985), 191–220.
[8] H. HASSE, Neue bergründung der komplexen multiplikation, Teil I, J. für Math. 157 (1927), 115–139, Teil II, ibid. 165 (1931), 64–88.
[9] H. Y. JUNG, J. K. KOO AND D. H. SHIN, Generation of ray class field by elliptic units, Bull. Lond. Math. Soc. 41 (2009), 935–942.
[10] J. K. KOO AND D. H. SHIN, On some arithmetic properties of Siegel functions, Math. Zeit. 264 (2010), 137–177.
[11] D. KUBERT AND S. LANG, Modular units, Grundlehren der mathematischen Wissenschaften 244, Spinger-Verlag, New York-Berlin, 1981.
[12] S. LANG, Elliptic functions, With an appendix by J. Tate, 2nd edition, Grad. Texts in Math. 112, Spinger-Verlag, New York, 1987.
[13] K. RAMACHANDRA, Some applications of Kronecker's limit formula, Ann. of Math. (2) 80 (1964), 104–148.
[14] R. SCHERTZ, Construction of ray class fields by elliptic units, J. Théor. Nombres Bordeaux 9 (1997), 383–394.
[15] G. SHIMURA, Introduction to the arithmetic theory of automorphic functions, Iwanami Shoten and Princeton University Press, Princeton, N.J., 1971.
[16] J. H. SILVERMAN, Advanced topics in the arithmetic of elliptic curves, Grad. Texts in Math. 151, Springer-Verlag, New York, 1994.
[17] P. STEVENHAGEN, Hilbert's 12th problem, complex multiplication and Shimura reciprocity, Class field theory-its centenary and prospect (Tokyo, 1998), 161–176, Adv. Stud. Pure Math. 30, Math. Soc. Japan, Tokyo, 2001.

DEPARTMENT OF MATHEMATICAL SCIENCES
KAIST
DAEJEON 373–1
KOREA

E-mail addresses: DOSAL@kaist.ac.kr
: jkkoo@math.kaist.ac.kr
: shakur01@kaist.ac.kr