GENERATION OF CLASS FIELDS BY SIEGEL-RAMACHANDRA INVARIANTS

JA KYUNG KOO AND DONG HWA SHIN

Abstract. Let K be an imaginary quadratic field and $\mathfrak{f}$ be a nontrivial integral ideal of K. We show that the Siegel-Ramachandra invariant could be a primitive generator of the ray class field modulo $\mathfrak{f}$ over K (or, over the Hilbert class field of K).

1. Introduction

Let K be an imaginary quadratic field. For a nonzero integral ideal $\mathfrak{f}$ of K we denote by $\mathrm{Cl}(\mathfrak{f})$ the ray class group modulo $\mathfrak{f}$ and write C_0 for its unit class. Then, there exists an abelian extension of K whose Galois group is isomorphic to $\mathrm{Cl}(\mathfrak{f})$ via the Artin map by class field theory ([5] or [12]). The field, denoted by $K_\mathfrak{f}$, is called the *ray class field modulo* $\mathfrak{f}$ *of* K. In particular, the ray class field modulo $\mathcal{O}_K$ is called the *Hilbert class field of* K and is simply written as H_K.

For $(r_1, r_2) \in \mathbb{Q}^2 - \mathbb{Z}^2$, the *Siegel function* $g_{(r_1,r_2)}(\tau)$ on the complex upper half-plane $\mathfrak{H} = \{\tau \in \mathbb{C} : \mathrm{Im}(\tau) > 0\}$ is defined by

$$g_{(r_1,r_2)}(\tau) = -q^{\frac{1}{2}\mathbf{B}_2(r_1)} e^{\pi i r_2 (r_1-1)} (1-q_z) \prod_{n=1}^{\infty} (1-q^n q_z)(1-q^n q_z^{-1}) \tag{1.1}$$

where $\mathbf{B}_2(X) = X^2 - X + 1/6$ is the second Bernoulli polynomial, $q = e^{2\pi i\tau}$ and $q_z = e^{2\pi i z}$ with $z = r_1\tau + r_2$. If $\mathfrak{f}$ is nontrivial (that is, $\neq \mathcal{O}_K$) and $C \in \mathrm{Cl}(\mathfrak{f})$, then we take any integral ideal $\mathfrak{c}$ in C so that $\mathfrak{f}\mathfrak{c}^{-1} = [z_1,\ z_2]$ $(= \mathbb{Z}z_1 + \mathbb{Z}z_2)$ with $z = z_1/z_2 \in \mathfrak{H}$. Now we define the *Siegel-Ramachandra invariant* (of conductor $\mathfrak{f}$ at C) by

$$g_\mathfrak{f}(C) = g^{12N}_{(\frac{a}{N},\ \frac{b}{N})}(z) \tag{1.2}$$

where N is the smallest positive integer in $\mathfrak{f}$ and a, b are integers such that $1 = (a/N)z_1 + (b/N)z_2$. This value depends only on the class C and lies in $K_\mathfrak{f}$. Furthermore, we have a well-known transformation formula

$$g_\mathfrak{f}(C_1)^{\sigma(C_2)} = g_\mathfrak{f}(C_1C_2) \quad (C_1,\ C_2 \in \mathrm{Cl}(\mathfrak{f})) \tag{1.3}$$

where σ is the Artin map ([10] Chapter 11 §1).

Ramachandra ([14]) constructed a primitive generator of $K_\mathfrak{f}$ over K for any nontrivial $\mathfrak{f}$ in terms of certain elliptic unit, but his invariant involves overly complicated product of Siegel-Ramachandra invariants and singular values of the modular Δ-function. Thus, Lang ([13] p. 292) and Schertz ([15]) conjectured that the simplest invariant $g_\mathfrak{f}(C_0)$ is a primitive generator of $K_\mathfrak{f}$ over K (or, over H_K), and Schertz conditionally proved the assertion. Recently, Jung et al. ([6]) proved that if $K \neq \mathbb{Q}(\sqrt{-1})$, $\mathbb{Q}(\sqrt{-3})$ and $\mathfrak{f} = (N)$ $(= N\mathcal{O}_K)$ for an integer N (≥ 2), then $g_\mathfrak{f}(C_0)$ generates $K_\mathfrak{f}$ over H_K by showing that $|g_\mathfrak{f}(C_0)| < |g_\mathfrak{f}(C_0)^\sigma|$ for all nonidentity element $\sigma \in \mathrm{Gal}(K_\mathfrak{f}/H_K)$.

In this paper we shall first give another proof of a weak version of the result of Jung et al., namely, for a given integer N (≥ 2), $g_{(N)}(C_0)$ generates $K_{(N)}$ over H_K except for $N^7/2$ imaginary quadratic fields K (Theorem 3.3). Furthermore, we shall develop a simple criterion of $\mathfrak{f}$ for $g_\mathfrak{f}(C_0)$ to be a primitive generator of $K_\mathfrak{f}$ over K by adopting Schertz's idea (Theorem 4.3 and Remark 4.4). In the last section we shall give some applications when $\mathfrak{f} = (2)$ (Proposition 5.4 and Theorem 5.6).

2010 *Mathematics Subject Classification.* 11F11, 11G15, 11R37.
Key words and phrases. class field theory, complex multiplication, modular forms.
The research was partially supported by Basic Science Research Program through the NRF of Korea funded by MEST (2010-0001654).

2. Preliminaries

In this section we shall review basic properties of Siegel functions and Shimura's reciprocity law.

For each positive integer N let $\mathcal{F}_N$ be the field of meromorphic modular functions of level N whose Fourier coefficients belong to the N^{th} cyclotomic field $\mathbb{Q}(e^{2\pi i/N})$. Then $\mathcal{F}_N$ is a Galois extension of $\mathcal{F}_1=\mathbb{Q}(j(\tau))$, where

$$j(\tau)=q^{-1}+744+196884q+21493760q^2+\cdots$$

is the modular j-function, whose Galois group $\mathrm{Gal}(\mathcal{F}_N/\mathcal{F}_1)$ is represented by $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1_2\}$ ([13] Chapter 6 Theorem 3).

Let $g(\tau)$ be an element of $\mathcal{F}_N$. If both $g(\tau)$ and $g(\tau)^{-1}$ are integral over $\mathbb{Q}[j(\tau)]$, then $g(\tau)$ is called a *modular unit* (of level N) . As is well-known, $g(\tau)$ is a modular unit if and only if it has no zeros and poles on $\mathfrak{H}$ ([10] Chapter 2 §2).

Proposition 2.1. *Let $(r_1,r_2)\in\frac{1}{N}\mathbb{Z}^2-\mathbb{Z}^2$ for some integer N (≥ 2).*

(i) *We have the order formula*

$$\mathrm{ord}_q\ g_{(r_1,r_2)}(\tau)=\frac{1}{2}\mathbf{B}_2(\langle r_1\rangle)$$

where $\langle r_1\rangle$ is the fractional part of r_1 in the interval $[0,1)$.

(ii) *$g_{(r_1,r_2)}^{12N/\gcd(6,N)}(\tau)$ is a modular unit of level N.*

(iii) *Furthermore, $\begin{pmatrix}a&b\\c&d\end{pmatrix}\in\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1_2\}\simeq\mathrm{Gal}(\mathcal{F}_N/\mathcal{F}_1)$ acts on $g_{(r_1,r_2)}^{12N/\gcd(6,N)}(\tau)$ by*

$$g_{(r_1,r_2)}^{12N/\gcd(6,N)}(\tau)^{\left(\begin{smallmatrix}a&b\\c&d\end{smallmatrix}\right)}=g_{(r_1,r_2)\left(\begin{smallmatrix}a&b\\c&d\end{smallmatrix}\right)}^{12N/\gcd(6,N)}(\tau)=g_{(r_1a+r_2c,r_1b+r_2d)}^{12N/\gcd(6,N)}(\tau).$$

Proof. (i) See [10] p. 31.
(ii) See [10] Chapter 3 Theorems 5.2 and 5.3.
(iii) See [13] Chapter 6 Theorem 3, [10] Chapter 2 Proposition 1.3 and [9] Proposition 2.4. □

Remark 2.2. Note that (iii) implies that $g_{(r_1,r_2)}^{12N/\gcd(6,N)}(\tau)$ is determined by $\pm(r_1,r_2)\mod\mathbb{Z}^2$.

In the following two propositions we let K be an imaginary quadratic field with discriminant d_K and

$$\theta_K=\begin{cases}\sqrt{d_K}/2 & \text{if } d_K\equiv 0\pmod 4\\ (-1+\sqrt{d_K})/2 & \text{if } d_K\equiv 1\pmod 4,\end{cases}\tag{2.1}$$

which generates $\mathcal{O}_K$ over $\mathbb{Z}$.

Proposition 2.3 (Main theorem of complex multiplication)**.** *For every positive integer N we have*

$$K_{(N)}=K\mathcal{F}_N(\theta_K)=K\big(h(\theta_K)\ :\ h\in\mathcal{F}_N\ \textit{is defined and finite at}\ \theta_K\big).$$

Proof. See [13] Chapter 10 Corollary to Theorem 2 or [16] Chapter 6. □

Furthermore, we have the following explicit description of Shimura's reciprocity law due to Stevenhagen which connects the class field theory with the theory of modular functions.

Proposition 2.4 (Shimura's reciprocity law)**.** *Let $\min(\theta_K,\ \mathbb{Q})=X^2+BX+C\in\mathbb{Z}[X]$. For each positive integer N the matrix group*

$$G_{K,N}=\left\{\begin{pmatrix}t-Bs&-Cs\\s&t\end{pmatrix}\in\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})\ :\ t,\ s\in\mathbb{Z}/N\mathbb{Z}\right\}$$

gives rise to the surjection

$$\begin{array}{ccl}G_{K,N}&\longrightarrow&\mathrm{Gal}(K_{(N)}/H_K)\\ \alpha&\mapsto&\big(h(\theta_K)\mapsto h^\alpha(\theta_K)\ :\ h(\tau)\in\mathcal{F}_N\ \textit{is defined and finite at}\ \theta_K\big)\end{array}$$

whose kernel is

$$\mathrm{Ker}_{K,N}=\begin{cases}\left\{\pm\begin{pmatrix}1&0\\0&1\end{pmatrix},\ \pm\begin{pmatrix}0&-1\\1&0\end{pmatrix}\right\} & \text{if } K=\mathbb{Q}(\sqrt{-1})\\ \left\{\pm\begin{pmatrix}1&0\\0&1\end{pmatrix},\ \pm\begin{pmatrix}-1&-1\\1&0\end{pmatrix},\ \pm\begin{pmatrix}0&-1\\1&1\end{pmatrix}\right\} & \text{if } K=\mathbb{Q}(\sqrt{-3})\\ \left\{\pm\begin{pmatrix}1&0\\0&1\end{pmatrix}\right\} & \text{otherwise.}\end{cases}$$

Proof. See [18] §3. □

3. Primitive generators over Hilbert class fields

Throughout this section we let K be an imaginary quadratic field and θ_K be as in (2.1). If $\mathfrak{f}=N\mathcal{O}_K$ for an integer N (≥ 2), then we get

$$g_{\mathfrak{f}}(C_0)=g^{12N}_{(0,\frac{1}{N})}(\theta_K)$$

by the definition (1.2).

Lemma 3.1. *Let* $(s,t)\in\mathbb{Z}^2-N\mathbb{Z}^2$ *for an integer* N *(*≥ 2*). If* $(s,t)\not\equiv\pm(0,1)\pmod N$*, then* $g^{12N}_{(0,\frac{1}{N})}(\tau)\neq g^{12N}_{(\frac{s}{N},\frac{t}{N})}(\tau)$.

Proof. Assume on the contrary that $g^{12N}_{(0,\frac{1}{N})}(\tau)=g^{12N}_{(\frac{s}{N},\frac{t}{N})}(\tau)$. Since

$$\mathrm{ord}_q\ g^{12N}_{(0,\frac{1}{N})}(\tau)=6N\mathbf{B}_2(0)=\mathrm{ord}_q\ g^{12N}_{(\frac{s}{N},\frac{t}{N})}(\tau)=6N\mathbf{B}_2(\langle\tfrac{s}{N}\rangle)$$

by Proposition 2.1(i), we must have $s\equiv 0\pmod N$ by the graph of $\mathbf{B}_2(X)=X^2-X+1/6$. Now, since

$$\begin{aligned}&\mathrm{ord}_q\left(g^{12N}_{(0,\frac{1}{N})}(\tau)^{\left(\begin{smallmatrix}0&-1\\1&0\end{smallmatrix}\right)}\right)=\mathrm{ord}_q\ g^{12N}_{(\frac{1}{N},0)}(\tau)=6N\mathbf{B}_2(\tfrac{1}{N})\\ =\ &\mathrm{ord}_q\left(g^{12N}_{(0,\frac{t}{N})}(\tau)^{\left(\begin{smallmatrix}0&-1\\1&0\end{smallmatrix}\right)}\right)=\mathrm{ord}_q\ g^{12N}_{(\frac{t}{N},0)}(\tau)=6N\mathbf{B}_2(\langle\tfrac{t}{N}\rangle)\end{aligned}$$

by Proposition 2.1(iii) and (i), it follows that $t\equiv\pm1\pmod N$. This proves the lemma. □

Lemma 3.2. (i) *$j(\tau)$ induces a bijective map* $j:\mathrm{SL}_2(\mathbb{Z})\backslash\mathfrak{H}\to\mathbb{C}$.

(ii) *If K_1 and K_2 are distinct imaginary quadratic fields, then θ_{K_1} and θ_{K_2} are not equivalent under the action of* $\mathrm{SL}_2(\mathbb{Z})$.

Proof. (i) See [13] Chapter 3 §3.
(ii) One can readily prove the assertion by observing the standard fundamental domain of $\mathrm{SL}_2(\mathbb{Z})\backslash\mathfrak{H}$ ([13] Chapter 3 §1). □

Theorem 3.3. *For a given integer N (≥ 2), $g^{12N}_{(0,\frac{1}{N})}(\theta_K)$ generates $K_{(N)}$ over H_K except for (less than) $N^7/2$ imaginary quadratic fields K.*

Proof. Let

$$S=\{(s,t)\in\mathbb{Z}^2\ :\ 0\leq s,\ t\leq N-1 \text{ and } (s,t)\neq(0,0),\ (0,1),\ (0,N-1)\}.$$

For each $(s,t)\in S$ we consider the function

$$g(\tau)=g^{12N}_{(0,\frac{1}{N})}(\tau)-g^{12N}_{(\frac{s}{N},\frac{t}{N})}(\tau)\quad(\in\mathcal{F}_N),$$

which is a zero of the polynomial

$$f(X)=\prod_{\rho\in\mathrm{Gal}(\mathcal{F}_N/\mathcal{F}_1)}(X-g(\tau)^\rho)=X^n+p_{n-1}(j(\tau))X^{n-1}+\cdots+p_0(j(\tau))$$

where $n=[\mathcal{F}_N:\mathcal{F}_1]$ and $p_{n-1}(X),\ \cdots,\ p_0(X)\in\mathbb{Q}(X)$. Note that $f(X)$ is a power of $\min(g(\tau),\mathcal{F}_1)$ and $p_0(X)\neq 0$ because $g(\tau)\neq 0$ by Lemma 3.1. Furthermore, since $g(\tau)$ is integral over $\mathbb{Q}[j(\tau)]$ by Proposition 2.1(ii), $p_{n-1}(X),\cdots,p_0(X)$ are polynomials over $\mathbb{Q}$. Let

$$Z_{(s,t)}=\{\text{imaginary quadratic fields } K\ :\ g(\theta_K)=0\}.$$

If K belongs to this set, then we get $p_0(j(\theta_K))=0$, since $g(\tau)$ is a zero of $f(X)$ and $j(\tau)$ is holomorphic on $\mathfrak{H}$. Hence we obtain $|Z_{(s,t)}|\leq\deg p_0(X)$ by Lemma 3.2(i) and (ii). On the other hand, any conjugate of $g(\tau)$ under the action of $\mathrm{Gal}(\mathcal{F}_N/\mathcal{F}_1)$ is of the form

$$g^{12N}_{(\frac{a}{N},\frac{b}{N})}(\tau)-g^{12N}_{(\frac{c}{N},\frac{d}{N})}(\tau)\quad((a,b),\ (c,d)\in\mathbb{Z}^2-N\mathbb{Z}^2)$$

by Proposition 2.1(iii). Since

$$\begin{aligned}\mathrm{ord}_q\big(g^{12N}_{(\frac{a}{N},\frac{b}{N})}(\tau)-g^{12N}_{(\frac{c}{N},\frac{d}{N})}(\tau)\big)&\geq\min\big\{6N\mathbf{B}_2(\langle\tfrac{a}{N}\rangle),\ 6N\mathbf{B}_2(\langle\tfrac{c}{N}\rangle)\big\}\quad\text{by Proposition 2.1(i)}\\&\geq 6N\mathbf{B}_2(\tfrac{1}{2})\quad\text{by the graph of }\mathbf{B}_2(X)=X^2-X+\frac{1}{6}\\&=-\frac{N}{2},\end{aligned}$$

we deduce that

$$\begin{aligned}\mathrm{ord}_q\ p_0(j(\tau))&=\mathrm{ord}_q\ \mathbf{N}_{\mathcal{F}_N/\mathcal{F}_1}(g(\tau))\\&\geq-\frac{N}{2}\cdot[\mathcal{F}_N:\mathcal{F}_1]=-\frac{N}{2}\cdot|\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1_2\}|\\&>-\frac{N}{2}\cdot N^4=-\frac{N^5}{2}.\end{aligned}$$

Thus we get $|Z_{(s,t)}|\leq\deg p_0(X)<N^5/2$ by the fact $\mathrm{ord}_q j(\tau)=-1$. It follows that if we let

$$Z=\bigcup_{(s,t)\in S}Z_{(s,t)},$$

then

$$|Z|\leq\sum_{(s,t)\in S}|Z_{(s,t)}|<\frac{N^5}{2}\cdot|S|<\frac{N^7}{2}.$$

Now, let K be an imaginary quadratic field not in Z. Suppose that $g^{12N}_{(0,\frac{1}{N})}(\theta_K)$ does not generate $K_{(N)}$ over H_K. Then there exists $\alpha=\begin{pmatrix}t-Bs&-Cs\\s&t\end{pmatrix}\in G_{K,N}/\mathrm{Ker}_{K,N}$ $(\simeq\mathrm{Gal}(K_{(N)}/H_K))$ in Proposition 2.4 which fixes $g^{12N}_{(0,\frac{1}{N})}(\theta_K)$. Hence we derive that

$$0=g^{12N}_{(0,\frac{1}{N})}(\theta_K)-g^{12N}_{(0,\frac{1}{N})}(\theta_K)^{\alpha}=g^{12N}_{(0,\frac{1}{N})}(\theta_K)-(g^{12N}_{(0,\frac{1}{N})}(\tau)^{\alpha})(\theta_K)=g^{12N}_{(0,\frac{1}{N})}(\theta_K)-g^{12N}_{(\frac{s}{N},\frac{t}{N})}(\theta_K)$$

by Propositions 2.4 and 2.1(iii). But this implies that K belongs to $Z_{(s,t)}$ $(\subseteq Z)$, which yields a contradiction. Therefore, if K is an imaginary quadratic field not in a finite set Z, then $g^{12N}_{(0,\frac{1}{N})}(\theta_K)$ generates $K_{(N)}$ over H_K. This completes the proof. □

Remark 3.4. We permitted rather rough inequalities in the above proof because the theorem actually holds true for all K $(\neq\mathbb{Q}(\sqrt{-1}),\ \mathbb{Q}(\sqrt{-3}))$ and N (≥ 2) without any exception ([6]).

4. Primitive generators of ray class fields

In this section we shall show that Siegel-Ramachandra invariants play a role of primitive generators of ray class fields over imaginary quadratic fields under certain condition by utilizing Schertz's idea ([15]).

Throughout this section we let K be an imaginary quadratic field with discriminant d_K and $\mathfrak{f}$ be a nonzero integral ideal of K. For a character χ of $\mathrm{Cl}(\mathfrak{f})$ we let $\mathfrak{f}_\chi$ be the conductor of χ and χ_0 be the proper character of $\mathrm{Cl}(\mathfrak{f}_\chi)$ corresponding to χ. If $\mathfrak{f}$ is nontrivial (that is, $\neq \mathcal{O}_K$) and χ is a nontrivial character of $\mathrm{Cl}(\mathfrak{f})$, then we define the *Stickelberger element*

$$S_\mathfrak{f}(\chi, g_\mathfrak{f}) = \sum_{C\in\mathrm{Cl}(\mathfrak{f})} \chi(C)\log|g_\mathfrak{f}(C)|,$$

and the *L-function*

$$L_\mathfrak{f}(s,\chi) = \sum_{\mathfrak{a}} \frac{\chi(\text{class of }\mathfrak{a})}{\mathbf{N}_{K/\mathbb{Q}}(\mathfrak{a})^s} \qquad (s\in\mathbb{C})$$

where $\mathfrak{a}$ runs over all nonzero integral ideals of K prime to $\mathfrak{f}$. Then, from the second Kronecker limit formula we get the following proposition.

Proposition 4.1. *Let χ be a character of $\mathrm{Cl}(\mathfrak{f})$. If $\mathfrak{f}_\chi$ is nontrivial, then*

$$\prod_{\substack{\mathfrak{p}\,:\,\text{nonzero prime ideals of }K\\ \mathfrak{p}|\mathfrak{f},\ \mathfrak{p}\nmid\mathfrak{f}_\chi}} (1-\overline{\chi}_0(\mathfrak{p}))L_{\mathfrak{f}_\chi}(1,\chi_0) = \frac{\pi}{3w(\mathfrak{f})N(\mathfrak{f})\tau(\overline{\chi}_0)\sqrt{-d_K}} S_\mathfrak{f}(\overline{\chi}, g_\mathfrak{f})$$

where $w(\mathfrak{f})$ is the number of roots of unity in K which are $\equiv 1 \pmod{\mathfrak{f}}$, $N(\mathfrak{f})$ is the smallest positive integer in $\mathfrak{f}$ and

$$\tau(\overline{\chi}_0) = -\sum_{\substack{x\in\mathcal{O}_K\\ x \pmod{\mathfrak{f}}\\ \gcd(x\mathcal{O}_K,\mathfrak{f}_\chi)=\mathcal{O}_K}} \overline{\chi}_0(\textit{class of } x\gamma\mathfrak{d}_K\mathfrak{f}_\chi)e^{2\pi i \mathbf{Tr}_{K/\mathbb{Q}}(x\gamma)}$$

with $\mathfrak{d}_K$ the different of $K/\mathbb{Q}$ and γ any element of K such that $\gamma\mathfrak{d}_K\mathfrak{f}_\chi$ is an integral ideal relatively prime to $\mathfrak{f}$.

Proof. See [13] Chapter 22 Theorem 2 and [10] Chapter 11 Theorem 2.1. □

Remark 4.2. (i) The product factor $\prod_{\mathfrak{p}|\mathfrak{f},\ \mathfrak{p}\nmid\mathfrak{f}_\chi}\left(1-\overline{\chi}_0(\mathfrak{p})\right)$ is called the *Euler factor of* χ. If there is no prime ideal $\mathfrak{p}$ such that $\mathfrak{p}|\mathfrak{f}$ and $\mathfrak{p}\nmid\mathfrak{f}_\chi$, then it is understood to be 1.
(ii) As is well-known ([5] Chapter IV Proposition 5.7), $L_{\mathfrak{f}_\chi}(1,\chi_0)\neq 0$.

Theorem 4.3. *Let $\mathfrak{f}$ be a nontrivial integral ideal of K whose prime ideal factorization is*

$$\mathfrak{f} = \prod_{k=1}^n \mathfrak{p}_k^{e_k}.$$

Assume that

$$[K_\mathfrak{f} : K] > 2\sum_{k=1}^n [K_{\mathfrak{f}\mathfrak{p}_k^{-e_k}} : K]. \tag{4.1}$$

Then $g_\mathfrak{f}(C_0)$ generates $K_\mathfrak{f}$ over K.

Proof. Set $F = K(g_\mathfrak{f}(C_0))$. We derive that

$$\begin{aligned} &|\{\text{characters }\chi\text{ of }\mathrm{Gal}(K_\mathfrak{f}/K):\ \chi|_{\mathrm{Gal}(K_\mathfrak{f}/F)}\neq 1\}| \\ =\ &|\{\text{characters }\chi\text{ of }\mathrm{Gal}(K_\mathfrak{f}/K)\}| - |\{\text{characters }\chi\text{ of }\mathrm{Gal}(F/K)\}| \\ =\ &[K_\mathfrak{f}:K]-[F:K]. \end{aligned} \tag{4.2}$$

Furthermore, we have

$$\begin{aligned} & |\{\text{characters } \chi \text{ of } \mathrm{Gal}(K_{\mathfrak{f}}/K) \ : \ \mathfrak{p}_k \nmid \mathfrak{f}_\chi \text{ for some } k\}| \\ = & |\{\text{characters } \chi \text{ of } \mathrm{Gal}(K_{\mathfrak{f}}/K) \ : \ \mathfrak{f}_\chi | \mathfrak{f}\mathfrak{p}_k^{-e_k} \text{ for some } k\}| \\ \leq & \sum_{k=1}^{n} |\{\text{characters } \chi \text{ of } \mathrm{Gal}(K_{\mathfrak{f}\mathfrak{p}_k^{-e_k}}/K)\}| = \sum_{k=1}^{n} [K_{\mathfrak{f}\mathfrak{p}_k^{-e_k}} : K]. \end{aligned} \tag{4.3}$$

Now, suppose that F is properly contained in $K_{\mathfrak{f}}$. Then we get from the assumption (4.1) that

$$[K_{\mathfrak{f}} : K] - [F : K] = [K_{\mathfrak{f}} : K]\left(1 - \frac{1}{[K_{\mathfrak{f}} : F]}\right) > 2\sum_{k=1}^{n}[K_{\mathfrak{f}\mathfrak{p}_k^{-e_k}} : K]\left(1 - \frac{1}{2}\right) = \sum_{k=1}^{n}[K_{\mathfrak{f}\mathfrak{p}_k^{-e_k}} : K].$$

This, together with (4.2) and (4.3), implies that there exists a character χ of $\mathrm{Gal}(K_{\mathfrak{f}}/K)$ such that

$$\chi|_{\mathrm{Gal}(K_{\mathfrak{f}}/F)} \neq 1, \tag{4.4}$$

$$\mathfrak{p}_k | \mathfrak{f}_\chi \text{ for all } k = 1, \cdots, n. \tag{4.5}$$

Identifying $\mathrm{Cl}(\mathfrak{f})$ and $\mathrm{Gal}(K_{\mathfrak{f}}/K)$ via the Artin map, we obtain from Proposition 4.1 and (4.5) that

$$0 \neq L_{\mathfrak{f}_\chi}(1, \chi_0) = TS_{\mathfrak{f}}(\overline{\chi}, g_{\mathfrak{f}}) \tag{4.6}$$

for certain nonzero constant T. On the other hand, we achieve that

$$\begin{aligned} S_{\mathfrak{f}}(\overline{\chi}, g_{\mathfrak{f}}) &= \sum_{C \in \mathrm{Cl}(\mathfrak{f})} \overline{\chi}(C) \log |g_{\mathfrak{f}}(C_0)^C| \quad \text{by (1.3)} \\ &= \sum_{\substack{C_1 \in \mathrm{Gal}(K_{\mathfrak{f}}/K) \\ C_1 \ (\mathrm{mod}\ \mathrm{Gal}(K_{\mathfrak{f}}/F))}} \sum_{C_2 \in \mathrm{Gal}(K_{\mathfrak{f}}/F)} \overline{\chi}(C_1C_2) \log |g_{\mathfrak{f}}(C_0)^{C_1C_2}| \\ &= \sum_{C_1}\sum_{C_2} \overline{\chi}(C_1)\overline{\chi}(C_2) \log |(g_{\mathfrak{f}}(C_0)^{C_2})^{C_1}| \\ &= \sum_{C_1} \overline{\chi}(C_1) \log |g_{\mathfrak{f}}(C_0)^{C_1}| \left(\sum_{C_2} \overline{\chi}(C_2)\right) \quad \text{by the fact } g_{\mathfrak{f}}(C_0) \in F \\ &= 0 \quad \text{by (4.4)}, \end{aligned}$$

which contradicts (4.6). Therefore, we conclude that $F = K_{\mathfrak{f}}$ as desired. □

Remark 4.4. For a nontrivial integral ideal $\mathfrak{f}$ of K we have a degree formula

$$[K_{\mathfrak{f}} : K] = \frac{h_K \varphi(\mathfrak{f}) w(\mathfrak{f})}{w_K} \tag{4.7}$$

where h_K is the class number of K, φ is the Euler function for ideals, namely

$$\varphi(\mathfrak{p}^n) = \big(\mathbf{N}_{K/\mathbb{Q}}(\mathfrak{p}) - 1\big)\mathbf{N}_{K/\mathbb{Q}}(\mathfrak{p})^{n-1}$$

for a prime ideal power $\mathfrak{p}^n$ ($n \geq 1$), $w(\mathfrak{f})$ is the number of roots of unity in K which are $\equiv 1 \pmod{\mathfrak{f}}$ and w_K is the number of roots of unity in K ([12] Chapter VI Theorem 1).

Let N (≥ 2) be an integer whose prime factorization is given by

$$N = \prod_{a=1}^{A} p_a^{u_a} \prod_{b=1}^{B} q_b^{v_b} \prod_{c=1}^{C} r_c^{w_c} \quad (A,\ B,\ C \geq 0,\ u_a,\ v_b,\ w_c > 0)$$

where each p_a (respectively, q_b and r_c) splits (respectively, is inert and ramified) in K. One can readily verify that the condition

$$2\sum_{a=1}^{A} \frac{1}{(p_a - 1)p_a^{u_a - 1}} + \sum_{b=1}^{B} \frac{1}{(q_b^2 - 1)q_b^{2(v_b - 1)}} + \sum_{c=1}^{C} \frac{1}{(r_c - 1)r_c^{2w_c - 1}} < \frac{1}{2w_K}$$

implies the assumption (4.1) with $\mathfrak{f} = N\mathcal{O}_K$.

Remark 4.5. In a recent paper ([7]) Jung et al. showed that if $K \neq \mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-3})$ and $\mathfrak{f} = N\mathcal{O}_K$ ($N \geq 2$), then $g_\mathfrak{f}(C_0)$ is indeed a primitive generator of $K_\mathfrak{f}$ over K. They manipulated actions of $\mathrm{Gal}(H_K/K)$ and $\mathrm{Gal}(K_\mathfrak{f}/H_K)$ separately rather than working with actions of $\mathrm{Gal}(K_\mathfrak{f}/K)$ directly by (1.3). It is worth noting that $g_\mathfrak{f}(C_0)$ has the smallest absolute value among all other conjugates because the conjugates of a large power of $1/g_\mathfrak{f}(C_0)$ become a normal basis of $K_\mathfrak{f}$ over K ([8]).

5. Siegel-Ramachandra invariants of conductor 2

Let K be an imaginary quadratic field and θ_K be as in (2.1). If $\mathfrak{f} = 2\mathcal{O}_K$, then $g_\mathfrak{f}(C_0) = g^{24}_{(0,\frac{1}{2})}(\theta_K)$. Note that $g^{12}_{(0,\frac{1}{2})}(\theta_K)$, which is a square root of $g_\mathfrak{f}(C_0)$, also lies in $K_{(2)}$ by Propositions 2.1(ii) and 2.3. In this section we shall examine some applications of $g^{12}_{(0,\frac{1}{2})}(\theta_K)$.

By the definition (1.1) we have

$$\begin{aligned} g^{12}_{(0,\frac{1}{2})}(\tau) &= 2^{12} q \prod_{n=1}^{\infty} (1+q^n)^{24} \\ g^{12}_{(\frac{1}{2},0)}(\tau) &= q^{-\frac{1}{2}} \prod_{n=1}^{\infty} (1-q^{n-\frac{1}{2}})^{24} \\ g^{12}_{(\frac{1}{2},\frac{1}{2})}(\tau) &= -q^{-\frac{1}{2}} \prod_{n=1}^{\infty} (1+q^{n-\frac{1}{2}})^{24}. \end{aligned} \tag{5.1}$$

Obviously, the above functions are all distinct and nonconstant. We have the following useful identities:

Lemma 5.1. (i) $g^{12}_{(0,\frac{1}{2})}(\tau) g^{12}_{(\frac{1}{2},0)}(\tau) g^{12}_{(\frac{1}{2},\frac{1}{2})}(\tau) = -2^{12}$.

(ii)

$$j(\tau) = \frac{(g^{12}_{(0,\frac{1}{2})}(\tau)+16)^3}{g^{12}_{(0,\frac{1}{2})}(\tau)} = \frac{(g^{12}_{(\frac{1}{2},0)}(\tau)+16)^3}{g^{12}_{(0,\frac{1}{2})}(\tau)} = \frac{(g^{12}_{(\frac{1}{2},\frac{1}{2})}(\tau)+16)^3}{g^{12}_{(0,\frac{1}{2})}(\tau)}.$$

Proof. See [1] p. 256 and Theorem 12.17. □

Proposition 5.2. *Let K be an imaginary quadratic field of discriminant d_K and θ_K be as in (2.1).*

(i) *$j(\theta_K)$ is an algebraic integer which generates H_K over K.*

(ii) *If p is a prime dividing the discriminant of $\min(j(\theta_K), K)$, then $(\frac{d_K}{p}) \neq 1$ and $p \leq |d_K|$.*

Proof. (i) See [13] Chapter 5 Theorem 4 and Chapter 10 Theorem 1.
(ii) See [3] and [2]. □

Remark 5.3. (i) $g^{12}_{(0,\frac{1}{2})}(\tau)$, $g^{12}_{(\frac{1}{2},0)}(\tau)$ and $g^{12}_{(\frac{1}{2},\frac{1}{2})}(\tau)$ are (distinct) roots of the cubic equation

$$(X+16)^3 - j(\tau)X = 0$$

by Lemma 5.1(ii). Hence $g^{12}_{(0,\frac{1}{2})}(\theta_K)$, $g^{12}_{(0,\frac{1}{2})}(\theta_K) g^{12}_{(\frac{1}{2},0)}(\theta_K)$ and $g^{12}_{(0,\frac{1}{2})}(\theta_K) g^{12}_{(\frac{1}{2},\frac{1}{2})}(\theta_K)$ are all algebraic integers dividing 2^{12} by Proposition 5.2(i) and Lemma 5.1(i). Furthermore, one can easily check by (5.1) and the definition (2.1) that $g^{12}_{(0,\frac{1}{2})}(\theta_K)$ is always a real number, but $g^{12}_{(0,\frac{1}{2})}(\theta_K) g^{12}_{(\frac{1}{2},0)}(\theta_K)$ and $g^{12}_{(0,\frac{1}{2})}(\theta_K) g^{12}_{(\frac{1}{2},\frac{1}{2})}(\theta_K)$ are real numbers when $d_K \equiv 0 \pmod 4$.

(ii) In [9] authors showed in general that if $(r_1, r_2) \in \frac{1}{N}\mathbb{Z}^2 - \mathbb{Z}^2$ for some integer N (≥ 2), then $g_{(r_1,r_2)}(\tau)$ is integral over $\mathbb{Z}[j(\tau)]$. Hence $g_{(r_1,r_2)}(\theta_K)$ is an algebraic integer by Proposition 5.2(i).

Proposition 5.4. *Let K ($\neq \mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-3})$) be an imaginary quadratic field of discriminant $d_K \equiv 1 \pmod 8$ or $\equiv 0 \pmod 4$, and θ_K be as in (2.1). Set $x = \mathbf{N}_{K_{(2)}/H_K}(g^{12}_{(0,\frac{1}{2})}(\theta_K))$.*

(i) *x is a (nonzero) real algebraic integer dividing 2^{12} which generates H_K over K. And, $\min(x, K)$ has integer coefficients.*

(ii) *If p is an odd prime dividing the discriminant of* $\min(x,K)$*, then* $(\frac{d_K}{p})\neq 1$ *and* $d\leq |d_K|$.

Proof. (i) We have

$$[K_{(2)}:H_K]=\begin{cases}1 & \text{if } d_K\equiv 1 \pmod 8\\ 2 & \text{if } d_K\equiv 0 \pmod 4\end{cases}$$

by (4.7), and

$$\mathrm{Gal}(K_{(2)}/H_K)\cong\begin{cases}\left\{\begin{pmatrix}1&0\\0&1\end{pmatrix}\right\} & \text{if } d_K\equiv 1 \pmod 8\\ \left\{\begin{pmatrix}1&0\\0&1\end{pmatrix},\begin{pmatrix}0&1\\1&0\end{pmatrix}\right\} & \text{if } d_K\equiv 4 \pmod 8\\ \left\{\begin{pmatrix}1&0\\0&1\end{pmatrix},\begin{pmatrix}1&0\\1&1\end{pmatrix}\right\} & \text{if } d_K\equiv 0 \pmod 8.\end{cases}$$

by Proposition 2.4. Hence we obtain

$$x=\mathbf{N}_{K_{(2)}/H_K}(g^{12}_{(0,\frac{1}{2})}(\theta_K))=\begin{cases}g^{12}_{(0,\frac{1}{2})}(\theta_K) & \text{if } d_K\equiv 1 \pmod 8\\ g^{12}_{(0,\frac{1}{2})}(\theta_K)g^{12}_{(\frac{1}{2},0)}(\theta_K) & \text{if } d_K\equiv 4 \pmod 8\\ g^{12}_{(0,\frac{1}{2})}(\theta_K)g^{12}_{(\frac{1}{2},\frac{1}{2})}(\theta_K) & \text{if } d_K\equiv 0 \pmod 8\end{cases}\tag{5.2}$$

by Propositions 2.4 and 2.1(iii). Note that x is a real algebraic integer dividing 2^{12} by Remark 5.3(i). It follows from Lemma 5.1 that

$$j(\theta_K)=\begin{cases}(x+16)^3/x & \text{if } d_K\equiv 1 \pmod 8\\ (256-x)^3/x^2 & \text{if } d_K\equiv 0 \pmod 4.\end{cases}\tag{5.3}$$

Therefore x generates H_K over K by Proposition 5.2(i). On the other hand, since x is a real number, we get

$$[K(x):K]=\frac{[K(x):\mathbb{Q}(x)]\cdot[\mathbb{Q}(x):\mathbb{Q}]}{[K:\mathbb{Q}]}=[\mathbb{Q}(x):\mathbb{Q}].$$

This implies that $\min(x,K)=\min(x,\mathbb{Q})$, which has integer coefficients because x is an algebraic integer.
(ii) If K has class number one, then there is nothing to prove. If σ_1 and σ_2 are distinct elements of $\mathrm{Gal}(H_K/K)$, then we derive from (5.3) that

$$\begin{aligned}&j(\theta_K)^{\sigma_1}-j(\theta_K)^{\sigma_2}\\ =&\begin{cases}(x_1-x_2)(x_1^2x_2+x_1x_2^2+48x_1x_2-4096)/x_1x_2 & \text{if } d_K\equiv 1 \pmod 8\\ (x_1-x_2)(-x_1^2x_2^2+196608x_1x_2-16777216x_1-16777216x_2)/x_1^2x_2^2 & \text{if } d_K\equiv 0 \pmod 4\end{cases}\end{aligned}$$

where $x_1=x^{\sigma_1}$ and $x_2=x^{\sigma_2}$. Note from Remark 5.3(i) that there is no prime ideal $\mathfrak{p}$ of H_K which contains x_1x_2 and lies above an odd prime. Therefore, if p is an odd prime dividing the discriminant of $\min(x,K)$, then $(\frac{d_K}{p})\neq 1$ and $|p|\leq d_K$ by Proposition 5.2(ii). □

Remark 5.5. If K ($\neq\mathbb{Q}(\sqrt{-3})$) is an imaginary quadratic field of discriminant $d_K\equiv 5 \pmod 8$, then one can readily verify that $\mathbf{N}_{K_{(2)}/H_K}(g^{12}_{(0,\frac{1}{2})}(\theta_K))=-2^{12}$ by Propositions 2.4, 2.1(iii) and Lemma 5.1(i). Hence one cannot develop Theorem 5.4 for $\mathbf{N}_{K_{(2)}/H_K}(g^{12}_{(0,\frac{1}{2})}(\theta_K))$ in this case.

By adopting the idea of the proof of Theorem 3.3 we can partially reprove Gauss' class number one problem for imaginary quadratic fields.

Theorem 5.6. *There are only finitely many imaginary quadratic fields K of discriminant $d_K\equiv 1 \pmod 8$ or $\equiv 0 \pmod 4$ with class number one.*

Proof. Let K ($\neq \mathbb{Q}(\sqrt{-1}),\ \mathbb{Q}(\sqrt{-3})$) be such an imaginary quadratic field and θ_K be as in (2.1). Since $\mathbf{N}_{K_{(2)}/H_K}(g^{12}_{(0,\frac{1}{2})}(\theta_K))$ is a (nonzero) real algebraic integer dividing 2^{12} by Proposition 5.4(i), it should be one of $\pm 1,\ \pm 2^1,\ \pm 2^2,\ \cdots, \pm 2^{12}$. Consider the function

$$G(\tau) = \begin{cases} g^{12}_{(0,\frac{1}{2})}(\tau) & \text{if } d_K \equiv 1 \pmod 8 \\ -2^{12}/g^{12}_{(\frac{1}{2},\frac{1}{2})}(\tau) & \text{if } d_K \equiv 4 \pmod 8 \\ -2^{12}/g^{12}_{(\frac{1}{2},0)}(\tau) & \text{if } d_K \equiv 0 \pmod 8 \end{cases}$$

which belongs to $\mathcal{F}_2$ by Proposition 2.1(ii), and satisfies $G(\theta_K) = \mathbf{N}_{K_{(2)}/H_K}(g^{12}_{(0,\frac{1}{2})}(\theta_K))$ by Lemma 5.1(i) and (5.2). Since $G(\tau)$ is not a constant, there are only finitely many points τ_0 on the modular curve of level 2 such that $G(\tau_0) = \pm 1,\ \pm 2^1,\ \pm 2^2,\ \cdots, \pm 2^{12}$. It follows form Lemma 3.2(ii) that there are only finitely many imaginary quadratic fields K such that $G(\theta_K) = \pm 1,\ \pm 2^1,\ \pm 2^2,\ \cdots, \pm 2^{12}$. This proves the theorem. □

Remark 5.7. (i) By using (5.1) and the definition (2.1) one can directly show that $|G(\theta_K)| < 1$ if $d_K \leq -40$ ([17]). This fact gives another proof of Theorem 5.6.

(ii) In 1903, Landau ([11]) presented a simple proof of Theorem 5.6. The complete determination of imaginary quadratic fields of class number one was first accomplished by Heegner ([4]) in 1952.

References

1. D. A. Cox, *Primes of the form x^2+ny^2: Fermat, Class Field, and Complex Multiplication*, A Wiley-Interscience Publication, John Wiley & Sons, Inc., New York, 1989.
2. D. R. Dorman, *Singular moduli, modular polynomials, and the index of the closure of $\mathbb{Z}[j(\tau)]$ in $\mathbb{Q}(j(\tau))$*, Math. Ann. 283 (1989), no. 2, 177-191.
3. B. H. Gross and D. B. Zagier, *On singular moduli*, J. Reine Angew. Math. 355 (1985), 191-220.
4. K. Heegner, *Diophantische Analysis und Modulfunktionen*, Math. Zeit. 56 (1952), 227-253.
5. G. J. Janusz, *Algebraic Number Fields*, Academic Press, 1973.
6. H. Y. Jung, J. K. Koo and D. H. Shin, *Generation of ray class field by elliptic units*, Bull. Lond. Math. Soc. 41 (2009), no. 5, 935-942.
7. H. Y. Jung, J. K. Koo and D. H. Shin, *Ray class invariants over imaginary quadratic fields*, http://arxiv.org/abs/1007.2317, submitted.
8. H. Y. Jung, J. K. Koo and D. H. Shin, *Normal bases of ray class fields over imaginary quadratic fields*, http://arxiv.org/abs/1007.2312, submitted.
9. J. K. Koo and D. H. Shin, *On some arithmetic properties of Siegel functions*, Math. Zeit. 264 (2010), no. 1, 137-177.
10. D. Kubert and S. Lang, *Modular Units*, Grundlehren der mathematischen Wissenschaften 244, Spinger-Verlag, New York-Berlin, 1981.
11. E. Landau, *Über die Klassenzahl der binaren quadratischen Formen von negativer Discriminante*, Math. Ann. 56 (1903), no. 4, 671-676
12. S. Lang, *Algebraic Number Theory*, 2nd edition, Spinger-Verlag, New York, 1994.
13. S. Lang, *Elliptic Functions*, 2nd edition, Spinger-Verlag, New York, 1987.
14. K. Ramachandra, *Some applications of Kronecker's limit formula*, Ann. of Math. (2) 80 (1964), 104-148.
15. R. Schertz, *Construction of ray class fields by elliptic units*, J. Theor. Nombres Bordeaux 9 (1997), no. 2, 383-394.
16. G. Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions*, Iwanami Shoten and Princeton University Press, 1971.
17. D. H. Shin, *Arithmetic properties of Siegel functions and applications*, Ph. D. Thesis, KAIST (2010).
18. 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
Current address: Daejeon 373-1, Korea
E-mail address: jkkoo@math.kaist.ac.kr

Department of Mathematical Sciences, KAIST
Current address: Daejeon 373-1, Korea
E-mail address: shakur01@kaist.ac.kr