GENERATION OF CLASS FIELDS BY
SIEGEL-RAMACHANDRA INVARIANTS

DONG HWA SHIN

Abstract. We show in many cases that the Siegel-Ramachandra invariants generate the ray class fields over imaginary quadratic fields. As its application we revisit the class number one problem done by Heegner and Stark, and present a new proof by making use of inequality argument together with Shimura’s reciprocity law.

1. Introduction

Let $K$ be an imaginary quadratic field with the ring of integers $\mathcal{O}_K$. For a nontrivial ideal $\mathfrak{f}$ of $\mathcal{O}_K$, we denote by $\text{Cl}(\mathfrak{f})$ the ray class group modulo $\mathfrak{f}$ and write $C_0$ for its identity class. By class field theory there exists a unique abelian extension $K_{\mathfrak{f}}$ of $K$, called the ray class field modulo $\mathfrak{f}$, whose Galois group is isomorphic to $\text{Cl}(\mathfrak{f})$ via the Artin reciprocity map [10, Chapter V]. In particular, the ray class field modulo $\mathcal{O}_K$ is called the Hilbert class field of $K$ and is simply written by $H_K$.

For a rational pair $[r_1 \ r_2] \in \mathbb{Q}^2 \setminus \mathbb{Z}^2$, the Siegel function $g_{[r_1 \ r_2]}(\tau)$ on the complex upper half-plane $\mathbb{H} = \{\tau \in \mathbb{C} \mid \text{Im}(\tau) > 0\}$ is defined by

\[ g_{[r_1 \ r_2]}(\tau) = -q^{(1/2)}B_2(r_1)e^{\pi ir_2(r_1-1)}(1 - qz) \prod_{n=1}^{\infty} (1 - q^n q_z)(1 - q^n q_z^{-1}), \]

where $B_2(X) = X^2 - X + 1/6$ is the second Bernoulli polynomial, $q = e^{2\pi i \tau}$ and $q_z = e^{2\pi iz}$ with $z = r_1\tau + r_2$. It has neither zeros nor poles on $\mathbb{H}$. If $\mathfrak{f} \neq \mathcal{O}_K$ and $C \in \text{Cl}(\mathfrak{f})$, then we take any integral ideal $\mathfrak{c}$ in $C$ and $z_1, z_2 \in \mathbb{C}$ such that $\mathfrak{f}^{-1} = \mathbb{Z}z_1 + \mathbb{Z}z_2$ and $z = z_1/z_2 \in \mathbb{H}$. We then define the Siegel-Ramachandra
invariant modulo \( f \) at \( C \) by

\[
g_f(C) = g_{[a/N]}\left(\frac{1}{b/N}\right)(z)^{12N},
\]

where \( N \) is the smallest positive integer in \( f \) and \( a, b \) are integers such that

\[1 = \left(\frac{a}{N}\right)z_1 + \left(\frac{b}{N}\right)z_2.\]

This value depends only on the class \( C \) [12, Chapter 2, Remark to Theorem 1.2], and lies in \( K_f \) [12, Chapter 2, Proposition 1.3 and Chapter 11, Theorem 1.1]. Furthermore, it satisfies the transformation formula

\[
g_f(C_1)^{\sigma(C_2)} = g_f(C_1C_2) \quad (C_1, C_2 \in \text{Cl}(f)),
\]

where \( \sigma \) is the Artin reciprocity map [12, pp. 235–236].

In 1964 Ramachandra [17, Theorem 10] first constructed a primitive generator of \( K_f \) over \( K \) for any \( f \neq \mathcal{O}_K \), however, his invariant involves overly complicated product of Siegel-Ramachandra invariants and the singular values of the modular \( \Delta \)-function. Thus, Lang [15, p. 292] and Schertz [20, p. 386] conjectured that the simplest invariant \( g_f(C_0) \) would be a primitive generator of \( K_f \) over \( K \) (or, over \( H_K \)), and Schertz gave a conditional proof [20, Theorems 3 and 4].

In this paper we shall first show in §3 that when \( f = (N) \) for an integer \( N \geq 2 \), \( g_f(C_0) \) generates \( K_f(N) \) over \( H_K \) for almost all imaginary quadratic fields \( K \) (Theorem 3.3). We shall further develop a simple criterion for \( g_f(C_0) \) to be a primitive generator of \( K_f \) over \( K \) when \( f \) is just a nontrivial ideal of \( \mathcal{O}_K \) (Theorem 3.6 and Remark 3.7) by adopting Schertz’s idea. In §4 we shall investigate some properties of Siegel-Ramachandra invariants modulo 2.

Gauss’ class number one problem for imaginary quadratic fields was first solved by Heegner [9] in 1952. There was a gap in his proof which heavily relies on the singular values of the Weber functions, however, few years later complete proofs were found independently by Baker [1] and Stark [25]. Moreover, Stark [25] finally filled up the supposed gap in Heegner’s proof. In §5 as an application we shall introduce a new proof (Theorems 4.8 and 5.2) by using Siegel functions and Stevenhagen’s explicit description of Shimura’s reciprocity law [26, §3, 6].

2. Preliminaries

First, we shall briefly review necessary basic properties of Siegel functions and Shimura’s reciprocity law.

For a positive integer \( N \) let \( \zeta_N = e^{2\pi i/N} \) be a primitive \( N \)-th root of unity and

\[
\Gamma(N) = \{ \gamma \in \text{SL}_2(\mathbb{Z}) \mid \gamma \equiv I_2 \pmod{N} \}
\]

be the principal congruence subgroup of level \( N \) of \( \text{SL}_2(\mathbb{Z}) \). Then its corresponding modular curve of level \( N \) is denoted by \( X(N) = \Gamma(N)\backslash(\mathbb{H} \cup \mathbb{P}^1(\mathbb{Q})) \).

Furthermore, we let \( \mathcal{F}_N \) be the field of meromorphic functions on \( X(N) \) defined
over the $N$-th cyclotomic field $\mathbb{Q}(\zeta_N)$. We know that $F_1 = \mathbb{Q}(j(\tau))$, where
\[
j(\tau) = q^{-1} + 744 + 196884q + 21493760q^2 + 864299970q^3 \\
+ 20245856256q^4 + \cdots
\]
is the elliptic modular $j$-function, and $F_N$ is a Galois extension of $F_1$ with
\[
\text{Gal}(F_N/F_1) \cong \text{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I_2\},
\]
whose action is given as follows: For an element $\alpha \in \text{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I_2\}$ we decompose it into
\[
\alpha = \alpha_1 \cdot \alpha_2
\]
for some $\alpha_1 \in \text{SL}_2(\mathbb{Z})$ and $\alpha_2 = \begin{bmatrix} 1 & 0 \\ 0 & d \end{bmatrix}$ with $d \in (\mathbb{Z}/N\mathbb{Z})^*$. Then, the action of $\alpha_1$ is given by a fractional linear transformation. And, $\alpha_2$ acts by the rule
\[
\sum_{n \gg -\infty} c_n q^{n/N} \mapsto \sum_{n \gg -\infty} c_{\sigma d}^n q^{n/N},
\]
where $\sum_{n \gg -\infty} c_n q^{n/N}$ is the Fourier expansion of a function in $F_N$ and $\sigma_d$ is the automorphism of $\mathbb{Q}(\zeta_N)$ defined by $\zeta_{\sigma d}^N = \zeta_N^d$ [15, Chapter 6, §3]. Here, for later use, we observe that
\[
[F_N:F_1] = \#\text{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I_2\} = \begin{cases} 6 & \text{if } N = 2, \\ (N^4/2) \prod_{p|N} (1 - p^{-1})(1 - p^{-2}) & \text{if } N \geq 3 \end{cases}
\]
[23, pp. 21–22].

**Proposition 2.1.** For a given integer $N \geq 2$ let \( \{m(r)\}_{r \in (1/N)\mathbb{Z}^2 \setminus \mathbb{Z}^2} \) be a family of integers such that $m(r) = 0$ except finitely many $r$. A product of Siegel functions
\[
g(\tau) = \zeta \prod_{r \in [r_1 \cdots r_2]} g_r(\tau)^{m(r)}
\]
belongs to $F_N$, where $\zeta = \prod_r e^{\pi i r (1-r_1)m(r)}$, if
\[
\sum_r m(r)(N r_1)^2 \equiv 0 \pmod{\gcd(2,N) \cdot N}, \\
\sum_r m(r)(N r_2)^2 \equiv 0 \pmod{\gcd(2,N) \cdot N}, \\
\gcd(12,N) \cdot \sum_r m(r) \equiv 0 \pmod{12}.
\]

**Proof.** See [12, Chapter 3, Theorems 5.2 and 5.3]. \qed

**Remark 2.2.** Let $g(\tau)$ be an element of $F_N$ for some integer $N \geq 2$. 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 neither zeros nor poles on $\mathbb{H}$ ([12, p. 36] or [11, Theorem 2.2]). Hence any product of
Siegel functions becomes a modular unit. In particular, \( g[r_1]^{12N/gcd(6,N)} \) is a modular unit of level \( N \) for any \([r_2] \in (1/N)\mathbb{Z}^2 \setminus \mathbb{Z}^2 \).

For a real number \( x \) we denote by \( \langle x \rangle \) the fractional part of \( x \) in the interval \([0,1)\).

**Proposition 2.3.** Let \([r_2] \in (1/N)\mathbb{Z}^2 \setminus \mathbb{Z}^2 \) for an integer \( N \geq 2 \).

(i) We have the \( q \)-order formula

\[
\text{ord}_q g[r_1](\tau) = \frac{1}{2} B_2((r_1)).
\]

(ii) For \( \gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \text{SL}_2(\mathbb{Z}) \) with \( c > 0 \) we get the transformation formula

\[
g[r_1](\tau) \circ \gamma = -i e^{(\pi i/6)(a/c+d/c-12\sum_{k=1}^{c-1}(k/c-1/2)(kd/c-1/2))} g[r_1a+rcd](\tau).
\]

(iii) For \( s = [x_2] \in \mathbb{Z}^2 \) we have

\[
g[r_1+s_1](\tau) = (-1)^{s_1+s_2+1} e^{-\pi i (s_1r_2-s_2r_1)} g[r_1](\tau).
\]

(iv) \( g[r_1](\tau)^{12N/gcd(6,N)} \) is determined only by \( \pm [r_2] \mod \mathbb{Z}^2 \).

(v) An element \( \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \text{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I_2\} \) acts on it by

\[
(g[r_1](\tau)^{12N/gcd(6,N)})^{[a \, b] \, [c \, d]} = g[r_1a+rcd](\tau)^{12N/gcd(6,N)}.
\]

(vi) \( g[r_1](\tau) \) is integral over \( \mathbb{Z}[j(\tau)] \).

**Proof.** (i) See [12, p. 31].

(ii) See [12, p. 27, K1 and p. 29] and [14, Chapter IX].

(iii) See [12, p. 28, K2 and p. 29].

(iv) One can easily check this relation by the definition (1) and (iii).

(v) See [12, Chapter 2, Proposition 1.3] and (iv).

(vi) See [11, §3].

For an imaginary quadratic field \( K \) of discriminant \( d_K \) we let

\[
\tau_K = \begin{cases} \sqrt{d_K}/2 & \text{if } d_K \equiv 0 \pmod{4}, \\ (3 + \sqrt{d_K})/2 & \text{if } d_K \equiv 1 \pmod{4}, \end{cases}
\]

which generates the ring of integers \( \mathcal{O}_K \) of \( K \) over \( \mathbb{Z} \). Then we have

\[
\min(\tau_K, \mathbb{Q}) = X^2 + BX + C = \begin{cases} X^2 - d_K/4 & \text{if } d_K \equiv 0 \pmod{4}, \\ X^2 - 3X + (9 - d_K)/4 & \text{if } d_K \equiv 1 \pmod{4}. \end{cases}
\]

For each positive integer \( N \) we define the matrix group

\[
W_{N, \tau_K} = \left\{ \begin{bmatrix} tBs \\ -Cs \\ t \end{bmatrix} \in \text{GL}_2(\mathbb{Z}/N\mathbb{Z}) \mid t, s \in \mathbb{Z}/N\mathbb{Z} \right\}.
\]
Proposition 2.4. For a positive integer $N$ we have
\[ K(N) = K(h(\tau_K)) \mid h \in \mathcal{F}_N \text{ is defined and finite at } \tau_K. \]

Proof. See [15, Chapter 10, Corollary to Theorem 2] or [23, Proposition 6.33]. □

Proposition 2.5 (Shimura’s reciprocity law). Let $K$ be an imaginary quadratic field. For each positive integer $N$, the matrix group $W_{N,\tau_K}$ gives rise to the surjection
\[ W_{N,\tau_K} \to \text{Gal}(K(N)/H_K) \]
\[ \alpha \mapsto (h(\tau_K) \mapsto h^\alpha(\tau_K) \mid h(\tau_K) \text{ is defined and finite at } \tau_K), \]
whose kernel is
\[ \text{Ker}_{N,\tau_K} = \begin{cases} \{ \pm \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \pm \begin{bmatrix} -1 & -3 \\ 1 & -2 \end{bmatrix}, \pm \begin{bmatrix} -2 & 3 \\ -1 & 1 \end{bmatrix} \} & \text{if } K = \mathbb{Q}(\sqrt{-3}), \\ \{ \pm \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \pm \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \} & \text{if } K = \mathbb{Q}(\sqrt{-1}), \\ \{ \pm \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \} & \text{otherwise.} \end{cases} \]

Proof. See [26, §3] or [7, pp. 50–51]. □

For an imaginary quadratic field $K$ of discriminant $d_K$, let
\[ C(d_K) = \{ aX^2 + bXY + cY^2 \in \mathbb{Z}[X,Y] \mid \gcd(a,b,c) = 1, b^2 - 4ac = d_K, \]
\[ (-a < b \leq c \text{ or } 0 \leq b \leq a = c) \}
be the form class group of reduced quadratic forms of discriminant $d_K$, whose identity element is
\[ \begin{cases} X^2 - (d_K/4)Y^2 \quad & \text{if } d_K \equiv 0 \pmod{4}, \\ X^2 + XY + ((1 - d_K)/4)Y^2 \quad & \text{if } d_K \equiv 1 \pmod{4} \end{cases} \]
[4, Theorems 2.8 and 3.9]. Note that if $aX^2 + bXY + cY^2 \in C(d_K)$, then
\[ a \leq \sqrt{|d_K|/3} \]
[4, p. 29] and the group $C(d_K)$ is isomorphic to the ideal class group of $K$, and hence to $\text{Gal}(H_K/K)$ [4, Theorem 7.7]. Thus, in particular, the class number of $K$ is the same as the order of the group $C(d_K)$, namely $[H_K : K]$. We denote it by $h_K$.

Proposition 2.6 (Shimura’s reciprocity law). Let $K$ be an imaginary quadratic field of discriminant $d_K$, and $p$ be a prime. For each $Q = aX^2 + bXY + cY^2 \in C(d_K)$ let
\[ \tau_Q = (-b + \sqrt{d_K})/2a \quad (\in \mathbb{Q}) \]
and $u_Q$ be an element of $\text{GL}_2(\mathbb{Z}/p\mathbb{Z})/\{ \pm I_2 \}$ given as follows:
Case 1. $d_K \equiv 0 \pmod{4}$

$$
\begin{cases}
\begin{bmatrix} a & b/2 \\ 0 & 1 \end{bmatrix} & \text{if } p \nmid a, \\
\begin{bmatrix} -b/2 & -c \\ 1 & 0 \end{bmatrix} & \text{if } p \mid a \text{ and } p \nmid c, \\
\begin{bmatrix} -a - b/2 & -c - b/2 \\ 1 & -1 \end{bmatrix} & \text{if } p \mid a \text{ and } p \mid c,
\end{cases}
$$

Case 2. $d_K \equiv 1 \pmod{4}$

$$
\begin{cases}
\begin{bmatrix} a & (3+b)/2 \\ 0 & 1 \end{bmatrix} & \text{if } p \nmid a, \\
\begin{bmatrix} (3-b)/2 & -c \\ 1 & 0 \end{bmatrix} & \text{if } p \mid a \text{ and } p \nmid c, \\
\begin{bmatrix} -a + (3-b)/2 & -(c + b)/2 \\ 1 & -1 \end{bmatrix} & \text{if } p \mid a \text{ and } p \mid c.
\end{cases}
$$

If $h(\tau) \in \mathcal{F}_p$ is defined and finite at $\tau_K$ and $h(\tau_K) \in H_K$, then the conjugates of $h(\tau_K)$ via the action of $\text{Gal}(H_K/K)$ are given by

$$
h^{u_Q}(\tau_Q) \quad (Q \in C(d_K))$$

possibly with some multiplicity.

**Proof.** See [26, §6] or [7, Lemma 20]. □

### 3. Generators of ray class fields

Let $K$ be an imaginary quadratic field. For an integer $N \geq 2$ we get

$$g_N(C_0) = g_{[0/1]}^{(\tau_K)^{12N}}$$

by the definition (2). In this section we shall show that it plays a role of primitive generator of $K_{(N)}$ over $H_K$ (or, even over $K$).

**Lemma 3.1.** Let $[\tau] \in \mathbb{Z}^2/N\mathbb{Z}^2$ for an integer $N \geq 2$. If $[\tau] \not\equiv \pm [1/1] \pmod{N}$, then $g_{[0/1]}^{(\tau)^{12N}} \neq g_{[s/N]}^{(\tau)^{12N}}$.

**Proof.** Assume on the contrary that $g_{[0/1]}^{(\tau)^{12N}} = g_{[s/N]}^{(\tau)^{12N}}$. Since

$$\text{ord}_q g_{[0/1]}^{(\tau)^{12N}} = 6NB_2(0) = \text{ord}_q g_{[s/N]}^{(\tau)^{12N}} = 6NB_2(s/N)$$

by Proposition 2.3(i), we must have $s \equiv 0 \pmod{N}$ by the graph of $B_2(X) = X^2 - X + 1/6$. And, since

$$\text{ord}_q g_{[0/1]}^{(\tau)^{12N}}[0 \ -1] = \text{ord}_q g_{[1/0]}^{(\tau)^{12N}} = 6NB_2(1/N)$$

It follows that $s \equiv 0 \pmod{N}$, which is a contradiction since $s \not\equiv 0 \pmod{N}$. □
\[ \text{ord}_q \left( g_{\frac{0}{t/N}}(\tau) \right)^{12N} \text{ord}_q - \text{ord}_q g_{\frac{t/N}{0}}(\tau)^{12N} = 6\text{NB}_2(t/N) \]

by Proposition 2.3(ii) and (i), it follows that \( t \equiv \pm 1 \pmod{N} \). This proves the lemma. \( \square \)

**Lemma 3.2.**

(i) \( j(\tau) \) induces a bijective map \( j : \text{SL}_2(\mathbb{Z}) \setminus \mathbb{H} \to \mathbb{C} \).

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

**Proof.** (i) See [15, Chapter 3, Theorem 4].

(ii) See [15, Chapter 3, Theorem 1]. \( \square \)

For a real number \( x \) we denote by \( \lfloor x \rfloor \) the greatest integer that is less than or equal to \( x \).

**Theorem 3.3.** For a given integer \( N \) (\( \geq 2 \) we have

\[
\# \left\{ \text{imaginary quadratic fields } K \mid g_{\frac{0}{1/N}}(\tau_K)^{12N} \text{ does not generate } K(N) \right\}
\]

\[
\leq \begin{cases} 
12 & \text{if } N = 2, \\
((N + 1)[N/2] - 1)(N^5/4) \prod_{p\mid N}(1 - p^{-1})(1 - p^{-2}) & \text{if } N \geq 3.
\end{cases}
\]

**Proof.** Let

\[ S = \left\{ \left[ \begin{smallmatrix} s \\ t \end{smallmatrix} \right] \in \mathbb{Z}^2 \mid (s = 0, \ 2 \leq t \leq [N/2]) \text{ or } (1 \leq s \leq [N/2], \ 0 \leq t \leq N - 1) \right\}, \]

which consists of \((N + 1)[N/2] - 1\) elements. For each \( \left[ \begin{smallmatrix} s \\ t \end{smallmatrix} \right] \in S \) we consider the function

\[ g(\tau) = g_{\frac{0}{1/N}}(\tau)^{12N} - g_{\frac{s/t}{N}}(\tau)^{12N} \in \mathcal{F}_N, \]

which is nonzero by Lemma 3.1. Since \( g(\tau) \) is integral over \( \mathbb{Z}[j(\tau)] \) by Proposition 2.3(vi), we have

\[ N_{\mathcal{F}_N/\mathcal{F}_1}(g(\tau)) = g(\tau) \prod_{\sigma \neq \text{id}} g(\tau)^\sigma = P(j(\tau)) \]

for some nonzero polynomial \( P(X) \in \mathbb{Z}[X] \).

Note by Proposition 2.3(v) that any conjugate of \( g(\tau) \) under the action of \( \text{Gal}(\mathcal{F}_N/\mathcal{F}_1) \) is of the form

\[ g_{[a/b]/N}(\tau)^{12N} \]

for some \( \left[ \begin{smallmatrix} a \\ b \end{smallmatrix} \right], \left[ \begin{smallmatrix} c \\ d \end{smallmatrix} \right] \in \mathbb{Z}^2 \setminus N\mathbb{Z}^2, \]

which is holomorphic on \( \mathbb{H} \). Now, let

\[ Z[\frac{1}{t}] = \{ \text{imaginary quadratic fields } K \mid g(\tau_K) = 0 \}. \]
If \( K \in \mathbb{Z}_{[\tau]} \), then (8) gives \( P(j(\tau_K)) = 0 \), from which we obtain by Lemma 3.2
\[
\# Z_{[\tau]} \leq \deg P(X).
\]
On the other hand, since
\[
\text{ord}_q \left( g\left[\frac{a}{N}\right]\left(\tau\right)^{12N} - g\left[\frac{c}{N}\right]\left(\tau\right)^{12N} \right)
\geq \min\{6NB_2((a/N)), 6NB_2((c/N))\} \text{ by Proposition 2.3(i)}
\geq 6NB_2(1/2) \text{ by the graph of } B_2(X) = X^2 - X + 1/6
= -N/2,
\]
we deduce that
\[
\text{ord}_q P(j(\tau)) = \text{ord}_q N_{F_n/F_1}(g(\tau))
\geq -(N/2) \cdot [F_N : F_1]
= -(N/2) \cdot \# \text{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I\}
= \begin{cases} 
-6 & \text{if } N = 2, \\
-(N^5/4) \prod_{p|N}(1-p^{-1})(1-p^{-2}) & \text{if } N \geq 3
\end{cases}
\text{ by (5)}.
\]
Thus we get from the fact \( \text{ord}_q j(\tau) = -1 \) that
\[
\# Z_{[\tau]} \leq \deg P(X) \leq \begin{cases} 
6 & \text{if } N = 2, \\
(N^5/4) \prod_{p|N}(1-p^{-1})(1-p^{-2}) & \text{if } N \geq 3
\end{cases}
\text{ by (6)}.
\]
And, if we let
\[
Z = \bigcup_{[\tau] \in S} Z_{[\tau]},
\]
then
\[
\# Z \leq \sum_{[\tau] \in S} \# Z_{[\tau]} \leq \# S \cdot \max_{[\tau] \in S} \{ \# Z_{[\tau]} \}
\leq \begin{cases} 
12 & \text{if } N = 2, \\
((N + 1)[N/2] - 1)(N^5/4) \prod_{p|N}(1-p^{-1})(1-p^{-2}) & \text{if } N \geq 3
\end{cases}
\text{ if } N = 2.
\]
Now, let \( K \) be an imaginary quadratic field lying outside \( Z \). Then the singular value \( g\left[\frac{0}{N}\right]\left(\tau_K\right)^{12N} \) generates \( K_{(N)} \) over \( H_K \). Indeed, suppose that it does not generate \( K_{(N)} \) over \( H_K \). Then there exists a non-identity element \( \alpha = \left[\frac{t-Bs-Cs}{t}\right] \) of \( W_{N,\tau_K}/\text{Ker}_{N,\tau_K} \) \( (\simeq \text{Gal}(K_{(N)}/H_K)) \) in Proposition 2.5 which fixes \( g\left[\frac{0}{N}\right]\left(\tau_K\right)^{12N} \). Here we may assume that \( [\tau] \) belongs to \( S \) because \( W_{N,\tau_K}/\text{Ker}_{N,\tau_K} \) is a subgroup or a quotient of \( \text{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I\} \). We derive that
\[
0 = g\left[\frac{0}{N}\right]\left(\tau_K\right)^{12N} - (g\left[\frac{0}{N}\right]\left(\tau_K\right)^{12N})^\alpha.
\]
\[ g\left[ \frac{0}{1/N} \right] (\tau_K)^{12N} - g\left[ \frac{0}{1/N} \right] (\tau_K)^{12N} \] by Proposition 2.5
\[ = g\left[ \frac{0}{1/N} \right] (\tau_K)^{12N} - g\left[ \frac{s/N}{t/N} \right] (\tau_K)^{12N} \] by Proposition 2.3(iv) and (v).

But this implies that \( K \) belongs to \( Z_{[s]} (\subseteq Z) \), which yields a contradiction. Therefore we conclude that
\[ \{ \text{imaginary quadratic fields } K \mid g\left[ \frac{0}{1/N} \right] (\tau_K)^{12N} \text{ does not generate } K_{(N)} \text{ over } H_K \} \subseteq Z. \]

This completes the proof. \( \square \)

Let \( K \) be an imaginary quadratic field and \( \mathfrak{f} \) be a nontrivial ideal of \( \mathcal{O}_K \). For a character \( \chi \) of \( \text{Cl} (\mathfrak{f}) \) we let \( \mathfrak{f} \chi \) be the conductor of \( \chi \) and \( \chi_0 \) be the proper character of \( \text{Cl} (\mathfrak{f}) \) corresponding to \( \chi \). If \( \mathfrak{f} \neq \mathcal{O}_K \) and \( \chi \) is also a nontrivial character of \( \text{Cl} (\mathfrak{f}) \), then we define the Stickelberger element
\[ S_{\mathfrak{f}} (\chi, g_{\mathfrak{f}}) = \sum_{\mathfrak{C} \in \text{Cl} (\mathfrak{f})} \chi(\mathfrak{C}) \log |g_{\mathfrak{f}}(\mathfrak{C})|, \]
and the \( L \)-function
\[ L_{\mathfrak{f}} (s, \chi) = \sum_{\mathfrak{a}} \frac{\chi([\mathfrak{a}])}{N_{\mathcal{O}_K/\mathcal{O}(\mathfrak{a})}^s} \quad (s \in \mathbb{C}), \]
where \( \mathfrak{a} \) runs over all nontrivial ideals of \( \mathcal{O}_K \) relatively prime to \( \mathfrak{f} \) and \([\mathfrak{a}]\) is the class containing \( \mathfrak{a} \).

**Proposition 3.4** (The second Kronecker limit formula). If \( \mathfrak{f} \chi \neq \mathcal{O}_K \), then we have
\[ L_{\mathfrak{f}_\chi} (1, \chi_0) \prod_{\mathfrak{p} \nmid \mathfrak{f}_\chi} (1 - \chi_0([p])) = -\frac{\pi \chi_0([\gamma_{\mathcal{O}_K}])}{3N(\chi_0)^{\gamma/\omega(\mathfrak{f}_\chi)}} \text{S}_{\mathfrak{f}} (\chi_0, g_{\mathfrak{f}}), \]
where \( \gamma_{\mathcal{O}_K} \) is the different of \( \mathcal{O}_K/\mathcal{O} \), \( \gamma \) is a nonzero element of \( K \) so that \( \gamma_{\mathcal{O}_K} \chi_0 \) becomes an ideal of \( \mathcal{O}_K \) relatively prime to \( \mathfrak{f}_\chi \), \( N(\mathfrak{f}_\chi) \) is the smallest positive integer in \( \mathfrak{f}_\chi \), \( \omega(\mathfrak{f}_\chi) = |\{ \zeta \in \mathcal{O}_K^\times \mid \zeta \equiv 1 \pmod{\mathfrak{f}_\chi} \}| \) and
\[ T_{\gamma, \chi_0} = \sum_{x + \mathfrak{f}_\chi \in \mathcal{O}_K^\times} \chi_0([x \mathcal{O}_K]) e^{2\pi i \text{Tr}_{\mathcal{O}_K/\mathcal{O}} (x \gamma)}. \]

**Proof.** See [15, Chapter 22, Theorems 1 and 2] and [12, Chapter 11, Theorem 2.1]. \( \square \)

**Remark 3.5.**
(i) The Euler factor \( \prod_{\mathfrak{p} \nmid \mathfrak{f}_\chi} (1 - \chi_0([p])) \) is understood to be 1 if there is no prime ideal \( \mathfrak{p} \) such that \( \mathfrak{p} \nmid \mathfrak{f} \) and \( \mathfrak{p} \nmid \mathfrak{f}_\chi \).

(ii) As is well-known, \( L_{\mathfrak{f}_\chi} (1, \chi_0) \neq 0 \) [10, Chapter IV, Proposition 5.7].
**Theorem 3.6.** Let $K$ be an imaginary quadratic field and $\mathfrak{f}$ be a nontrivial proper ideal of $\mathcal{O}_K$ whose prime ideal factorization is given by

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

Assume that

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

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

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

$$\# \{ \text{characters } \chi \text{ of } \text{Gal}(K_\mathfrak{f}/K) \mid \chi|_{\text{Gal}(K_\mathfrak{f}/F)} \neq 1 \}$$

$$= \# \{ \text{characters } \chi \text{ of } \text{Gal}(K_\mathfrak{f}/K) \} - \# \{ \text{characters } \chi \text{ of } \text{Gal}(F/K) \}$$

$$= [K_\mathfrak{f} : K] - [F : K].$$

Furthermore, we have

$$\# \{ \text{characters } \chi \text{ of } \text{Gal}(K_\mathfrak{f}/K) \mid p_k \nmid f_\chi \text{ for some } k \}$$

$$= \# \{ \text{characters } \chi \text{ of } \text{Gal}(K_\mathfrak{f}/K) \mid f_\chi|p_k^{-e_k} \text{ for some } k \}$$

$$\leq \sum_{k=1}^{n} \# \{ \text{characters } \chi \text{ of } \text{Gal}(K_{p_k^{-e_k}}/K) \}$$

$$= \sum_{k=1}^{n} [K_{p_k^{-e_k}} : K].$$

Now, suppose that $F$ is properly contained in $K_\mathfrak{f}$. Then we get by the assumption (9) that

$$[K_\mathfrak{f} : K] - [F : K] = [K_\mathfrak{f} : K](1 - 1/[K_\mathfrak{f} : F])$$

$$> 2 \sum_{k=1}^{n} [K_{p_k^{-e_k}} : K](1 - 1/2)$$

$$= \sum_{k=1}^{n} [K_{p_k^{-e_k}} : K].$$

This, together with (10) and (11), implies that there exists a character $\chi$ of $\text{Gal}(K_\mathfrak{f}/K)$ such that

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

$$p_k \nmid f_\chi \text{ for all } k = 1, \ldots, n.$$
Identifying $\text{Cl}(f)$ and $\text{Gal}(K_f/K)$ via the Artin reciprocity map, we obtain from Proposition 3.4 and (13) that

\begin{equation}
0 \neq L_f(1, \chi_0) = -\frac{\pi \chi_0([\gamma \mathcal{D}_K f])}{3N(f)\sqrt{-d_K} \omega(f)T_f\chi_0} S_f(\chi, g_f).
\end{equation}

On the other hand, we achieve that

$$S_f(\chi, g_f) = \sum_{C \in \text{Cl}(f)} \chi(C) \log |g_f(C_0)^C| \quad \text{by (3)}$$

\begin{align*}
&= \sum_{C_1 \in \text{Gal}(K_f/K)} \sum_{C_2 \in \text{Gal}(K_f/F)} \n(C_1C_2) \log |g_f(C_0)^{C_1}| \\
&= \sum_{C_1} \sum_{C_2} \n(C_1) \n(C_2) \log |(g_f(C_0)^{C_2})^{C_1}| \\
&= \sum_{C_1} \n(C_1) \log |g_f(C_0)^{C_1}| \left(\sum_{C_2} \n(C_2)\right) \quad \text{by the fact } g_f(C_0) \in F \\
&= 0 \quad \text{by (12),}
\end{align*}

which contradicts (14). Therefore, we conclude $F = K_f$ as desired. \qed

Remark 3.7. (i) For a nontrivial integral ideal $f$ of an imaginary quadratic field $K$, we have a degree formula

\begin{equation}
[K_f : K] = \frac{h_K\varphi(f)\omega(f)}{\omega_K},
\end{equation}

where $\varphi$ is the (multiplicative) Euler function for ideals, namely

$$\varphi(p^n) = (N_{K/Q}(p) - 1)N_{K/Q}(p)^{n-1}$$

for a prime ideal power $p^n$ ($n \geq 1$), $\omega(f)$ is the number of roots of unity in $K$ which are $\equiv 1 \pmod{f}$ and $\omega_K$ is the number of roots of unity in $K$ [16, Chapter VI, Theorem 1].

Let $N (\geq 2)$ be an integer whose prime factorization is given by

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

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

$$4 \sum_{a=1}^{A} \frac{1}{p_a} + 2 \sum_{b=1}^{B} \frac{1}{q_b^{2v_b-1}} + 2 \sum_{c=1}^{C} \frac{1}{r_c^{2w_c-1}} < \frac{\omega((N))}{\omega_K}$$

implies the assumption (9) when $f = (N)$.

(ii) Let $d_k$ ($k = 1, \ldots, n$) be the exponent of the group $\left(O_K/p_k^{\infty}\right)^\times$. Schertz [20, Theorem 3] proved that if the conductor of the extension $K_f/K$ is exactly
then $g_l(C_0)$ is a primitive generator of $K_f$ over $K$ in either case when $n = 1$ or

\[ d_k \nmid 2 \quad (k = 1, \ldots, n - 1), \quad d_n \nmid 2\omega_K \text{ and } p_{\nu}^\infty \nmid \gcd(6, \omega_K). \]

Note that we do not require any condition on the conductor of the extension $K_f/K$.

4. Siegel-Ramachandra invariants of conductor 2

Throughout this section we let $K$ be an imaginary quadratic field. We shall examine certain properties of the singular value $g_{[0 \, 1/2]}(\tau_K)$ which is a 24-th root of $g_{[1/2]}(C_0)$. Although most of the results here are classical and known, we will present relatively short and new proofs purely in terms of Siegel functions.

By the definition \((1)\) we have

\[
g_{[0 \, 1/2]}(\tau) = 2\zeta_8 q^{1/12}\prod_{n=1}^{\infty} (1 + q^n)^2, \quad g_{[0 \, 1/2]}(\tau) = -q^{-1/24}\prod_{n=1}^{\infty} (1 - q^{n-1/2})^2, \quad \]

\[
g_{[1/2]}(\tau) = \zeta_8 q^{-1/24}\prod_{n=1}^{\infty} (1 + q^{n-1/2})^2. \]

Let $\gamma_2(\tau)$ be the cube root of $j(\tau)$ whose Fourier expansion begins with the term $q^{-1/3}$.

Lemma 4.1. (i) We have the identity

\[
g_{[0 \, 1/2]}(\tau)g_{[1/2]}(\tau)g_{[1/2]}(\tau) = 2\zeta_8. \]

(ii) We have the relations

\[
\gamma_2(\tau) = \frac{g_{[0 \, 1/2]}(\tau)^{12} + 16}{g_{[1/2]}(\tau)^4} = \frac{g_{[1/2]}(\tau)^{12} + 16}{g_{[1/2]}(\tau)^4} = \frac{g_{[1/2]}(\tau)^{12} + 16}{g_{[1/2]}(\tau)^4}. \]

Proof. (i) We obtain by \((17)\)

\[
g_{[0 \, 1/2]}(\tau)g_{[1/2]}(\tau)g_{[1/2]}(\tau) = 2\zeta_8 \prod_{n=1}^{\infty} (1 + q^n)^2(1 - q^{2n-1})^2 \]

\[
= 2\zeta_8 \prod_{n=1}^{\infty} \frac{(1 - q^{2n})^2}{(1 - q^n)^2} \frac{(1 - q^n)^2}{(1 - q^{2n})^2} = 2\zeta_8. \]

(ii) Since $g_{[0 \, 1/2]}(\tau)^{12} \in \mathcal{F}_2$ by Proposition 2.1 and

\[
\text{Gal}(\mathcal{F}_2/\mathcal{F}_1) \simeq \text{GL}_2(\mathbb{Z}/2\mathbb{Z})/\{\pm I_2\} \]
by (5), we derive that
\[
\prod_{\sigma \in \text{Gal}(F_2/F_1)} (X - (g_{[1/2]}(\tau)^{12})^\sigma)
= (X - g_{[1/2]}(\tau)^{12})^2(X - g_{[1/2]}(\tau)^{12})(X - g_{[1/2]}(\tau)^{12})^2
\]
by Proposition 2.3(iv) and (v)
\[
= (X^3 + 48X^2 + (-q^{-1} + 24 - 196884q + \cdots)X + 4096)^2 \quad \text{by (17)}
= (X^3 + 48X^2 + (-j(\tau) + 768X + 4096)^2 \quad \text{by (4)}
= ((X + 16)^3 - j(\tau)X)^2
= ((X + 16)^3 - \gamma_2(\tau)^3X)^2.
\]
Hence we get
\[
\gamma_2(\tau) = \xi_1 g_{[1/2]}(\tau)^{12} + 16 = \xi_2 g_{[1/2]}(\tau)^{12} + 16 = \xi_3 g_{[1/2]}(\tau)^{12} + 16
\]
for some cube roots of unity \(\xi_k \ (k = 1, 2, 3)\). Comparing the leading terms of Fourier expansions we conclude \(\xi_1 = \xi_2 = \xi_3 = 1\). \(\square\)

**Remark 4.2.** Let
\[
\eta(\tau) = \sqrt{2\pi} \zeta_8 q^{1/24} \prod_{n=1}^{\infty} (1 - q^n)
\]
be the Dedekind eta function, and
\[
f(\tau) = \zeta_8 q^{1/4} \frac{\eta((\tau + 1)/2)}{\eta(\tau)} , \quad f_1(\tau) = \frac{\eta(\tau/2)}{\eta(\tau)} , \quad f_2(\tau) = \sqrt{2} \frac{\eta(2\tau)}{\eta(\tau)}
\]
be the Weber functions. Then one can deduce the following identities
\[
(18) \quad f(\tau)^2 = \zeta_8^4 g_{[1/2]}(\tau) , \quad f_1(\tau)^2 = -g_{[1/2]}(\tau) , \quad f_2(\tau)^2 = \zeta_4^4 g_{[1/2]}(\tau),
\]
and hence Lemma 4.1(ii) can be reformulated in terms of the Weber functions as in the classical case [4, Theorem 12.17].

**Lemma 4.3.** If \(x\) is a real algebraic integer, then \(\min(x, K)\) has integer coefficients.

**Proof.** Since \(x \in \mathbb{R}\), we get
\[
[K(x) : K] = \frac{[K(x) : \mathbb{Q}(x)] \cdot [\mathbb{Q}(x) : \mathbb{Q}]}{[K : \mathbb{Q}]} = [\mathbb{Q}(x) : \mathbb{Q}],
\]
from which it follows that \(\min(x, K) = \min(x, \mathbb{Q})\). Furthermore, \(\min(x, K)\) has integer coefficients, because \(x\) is an algebraic integer. \(\square\)
Proposition 4.4. Let $K$ be an imaginary quadratic field of discriminant $d_K$.

(i) $j(\tau_K)$ is a real algebraic integer which generates $H_K$ over $K$.

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

Proof. (i) See [15, Chapter 5, Theorem 4 and Chapter 10, Theorem 1].

(ii) See [8], [6] or [4, Theorem 13.28]. □

Remark 4.5. For any $[r_1, r_2] \in \mathbb{Q}^2 \setminus \mathbb{Z}^2$, $g_{[r_1, r_2]}(\tau_K)$ is an algebraic integer by Propositions 2.3(vi) and 4.4(i).

Theorem 4.6. Let $K \neq \mathbb{Q}(\sqrt{-3}), \mathbb{Q}(\sqrt{-1})$ and set $x = N_{K(2)/H_K}(g_{[0, \frac{1}{2}]}(\tau_K)^{12})$.
Assume that 2 is not inert in $K$ (equivalently, $d_K \equiv 0 \pmod{4}$ or $d_K \equiv 1 \pmod{8}$).

(i) $x$ generates $H_K$ over $K$.

(ii) $x$ is a real algebraic integer dividing $2^{12}$ whose minimal polynomial $\min(x, K)$ has integer coefficients.

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

Proof. (i) Since $g_{[0, \frac{1}{2}]}(\tau)^{12} \in F_2$, $g_{[0, \frac{1}{2}]}(\tau_K)^{12}$ lies in $K(2)$ by Proposition 2.4.
Moreover, we have
\[
[K(2) : H_K] = \begin{cases} 
2 & \text{if } d_K \equiv 0 \pmod{4}, \\
1 & \text{if } d_K \equiv 1 \pmod{8},
\end{cases}
\]
by the degree formula (15), and
\[
\text{Gal}(K(2)/H_K) \simeq W_{2, \tau_K}/\text{Ker}_{2, \tau_K}
\]
\[
= \begin{cases} 
\left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \right\} & \text{if } d_K \equiv 0 \pmod{8}, \\
\left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \right\} & \text{if } d_K \equiv 4 \pmod{8}, \\
\left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \right\} & \text{if } d_K \equiv 1 \pmod{8},
\end{cases}
\]
by Proposition 2.5. So we obtain
\[
x = N_{K(2)/H_K}(g_{[0, \frac{1}{2}]}(\tau_K)^{12})
\]
\[
= \begin{cases} 
g_{[0, \frac{1}{2}]}(\tau_K)^{12}g_{[1/2]}(\tau_K)^{12} & \text{if } d_K \equiv 0 \pmod{8}, \\
g_{[0, \frac{1}{2}]}(\tau_K)^{12}g_{[1/2]}(\tau_K)^{12} & \text{if } d_K \equiv 4 \pmod{8}, \\
g_{[0, \frac{1}{2}]}(\tau_K)^{12} & \text{if } d_K \equiv 1 \pmod{8}
\end{cases}
\]
by Propositions 2.5 and 2.3(iv), (v); and hence

\[ j(\tau_K) = \begin{cases} 
(256 - x)^3/x^2 & \text{if } d_K \equiv 0 \pmod{4}, \\
(x + 16)^3/x & \text{if } d_K \equiv 1 \pmod{8}
\end{cases} \]

by Lemma 4.1. Therefore \( x \) generates \( H_K \) over \( K \) by Proposition 4.4(i).

(ii) We see that \( x < \mathbb{R} \) by the definition (7), (17) and (19). Furthermore, since \( x \) is an algebraic integer by Remark 4.5, \( \min(x, \sigma) \) has integer coefficients by Lemma 4.4. And, \( x \) divides \( 2^{12} \) by (19) and Lemma 4.1(i).

(iii) If \( h_K = 1 \), there is nothing to prove. So we assume \( h_K > 1 \). If \( \sigma_1 \) and \( \sigma_2 \) are distinct elements of \( \text{Gal}(H_K/K) \), then we derive from (20) that

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

where \( x_1 = x^{\sigma_1} \) and \( x_2 = x^{\sigma_2} \). Observe from (ii) that there is no prime ideal \( \mathfrak{p} \) of \( H_K \) which contains \( x_1 x_2 \) and lies above an odd prime. Therefore, if \( p \) is an odd prime dividing the discriminant of \( \min(x, \sigma) \), then \( (d_{\mathfrak{p}}) \neq 1 \) and \( p \leq |d_K| \) by Proposition 4.4(ii).

\[ \square \]

Remark 4.7. Let \( K \neq \mathbb{Q}(\sqrt{-3}), \mathbb{Q}(\sqrt{-1}) \). Since \( g_{[1/2]} \tau_K^{24} \) generates \( K_{(2)} \) over \( K \) by Theorem 3.6 and Remark 3.7, so does \( g_{[1/2]} \tau_K^{12} \). If \( 2 \) is inert in \( K \), then

\[ \text{Gal}(K_{(2)}/H_K) \cong W_{2, \tau_K}/\text{Ker}_{2, \tau_K} = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \right\} \]

by Proposition 2.5. And, we derive from Proposition 2.3(iv), (v) and Lemma 4.1(i) that

\[ N_{K_{(2)}/H_K}(g_{[1/2]} \tau_K^{12}) = g_{[1/2]} \tau_K^{12} g_{[0]} \tau_K^{12} g_{[1/2]} \tau_K^{12} = -2^{12}. \]

Therefore, in this case one cannot develop a theory like Theorem 4.6 with \( N_{K_{(2)}/H_K}(g_{[1/2]} \tau_K^{12}) \).

Theorem 4.8. Let \( K \) be an imaginary quadratic field of discriminant \( d_K \). Assume that \( 2 \) is inert and \( 3 \) is not ramified in \( K \) (equivalently, \( d_K \equiv 5 \pmod{8} \) and \( d_K \not\equiv 0 \pmod{3} \)).

(i) The real algebraic integer \( \zeta_8 g_{[0]} \tau_K \) generates \( K_{(2)} \) over \( H_K \).

(ii) The real algebraic integer \( \gamma_2 \tau_K \) generates \( H_K \) over \( K \).

Proof. (i) Let $\alpha = g_{1/2}(\tau_K)$. It is an algebraic integer by Remark 4.5, and $\zeta_8\alpha \in \mathbb{R}$ by the definition (7) and (17). Since $\alpha^4$ is a real cube root of $\alpha^{12}$, we get from Remark 4.7 that

$$[K_2(\alpha^4) : K_2] = [K(\alpha^4) : K(\alpha^{12})] = \frac{[K(\alpha^4) : \mathbb{Q}(\alpha^4)][\mathbb{Q}(\alpha^4) : \mathbb{Q}(\alpha^{12})]}{[K(\alpha^{12}) : \mathbb{Q}(\alpha^{12})]}$$

$$= [\mathbb{Q}(\alpha^4) : \mathbb{Q}(\alpha^{12})] = 1 \text{ or } 3.$$  

Furthermore, since $g_{1/2}(\tau) \in \mathcal{F}_8$ by Proposition 2.1, we get $\alpha^4 \in K_6$ by Proposition 2.4, from which it follows that $[K_2(\alpha^4) : K_2]$ divides

$$[K_6 : K_2] = \begin{cases} 2 & \text{if } 3 \text{ splits in } K, \\ 4 & \text{if } 3 \text{ is inert in } K \end{cases}$$

by the degree formula (15). Hence $[K_2(\alpha^4) : K_2] = 1$, which implies $\alpha^4 \in K_2$.

On the other hand, since $\zeta_8^{-1}g_{1/2}(\tau)^3 \in \mathcal{F}_8$ by Proposition 2.1, we obtain $\zeta_8^{-1}\alpha^3 \in K_8$ by Proposition 2.4. One can then readily check by Proposition 2.5 that

$$\text{Gal}(K_8/K_2) \cong \left\langle \begin{bmatrix} 5 & 4 \\ 4 & 1 \end{bmatrix} \right\rangle \times \left\langle \begin{bmatrix} 7 & 6 \\ 2 & 1 \end{bmatrix} \right\rangle \times \left\langle \begin{bmatrix} 7 & 2 \\ 2 & 1 \end{bmatrix} \right\rangle \text{ if } d_K \equiv 5 \text{ (mod 16)},$$

$$\cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}. \text{ if } d_K \equiv 13 \text{ (mod 16)}.$$  

Decomposing $[\frac{5}{1} \frac{4}{1}] = [\frac{5}{12} \frac{12}{29}] [\frac{1}{1} \frac{0}{1}]$, we deduce that

$$(\zeta_8^{-1} \alpha^3)^{[\frac{5}{1} \frac{4}{1}]} = (\zeta_8^{-1}g_{1/2}(\tau)^3)^{[\frac{5}{12} \frac{12}{29}] [\frac{1}{1} \frac{0}{1}]}(\tau_K) \text{ by Proposition 2.5}$$

$$= (\zeta_8^{-1}g_{1/2}(\tau)^3)^{[12 \frac{5}{12}] [\frac{1}{1} \frac{0}{1}]}(\tau_K)$$

$$= (\zeta_8^{-1}g_{12/29}(\tau)^3)^{[10 \frac{1}{2}]}(\tau_K) \text{ by Proposition 2.3(ii)}$$

$$= (\zeta_8^3g_{12/29}(\tau)^3)^{[10 \frac{1}{2}]}(\tau_K) \text{ by Proposition 2.3(iii)}$$

$$= (8\zeta_8q^{1/4} \prod_{n=1}^{\infty} (1 + q^n)^{[10 \frac{1}{2}]})(\tau_K) \text{ by (17)}$$

$$= (8\zeta_8^5q^{1/4} \prod_{n=1}^{\infty} (1 + q^n)^{[10 \frac{1}{2}]})$$

$$= \zeta_8^{-1}g_{1/2}(\tau)^3$$

$$= \zeta_8^{-1} \alpha^3.$$
In a similar way, one can verify that $\zeta_8^{-1}\alpha^3$ is invariant under the actions of
\[
\begin{bmatrix} 7 & 6 \\ 2 & 1 \end{bmatrix} = \begin{bmatrix} 7 & 2 \\ 10 & 3 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 3 \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} 7 & 2 \\ 2 & 1 \end{bmatrix} = \begin{bmatrix} 23 & 14 \\ 18 & 11 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 3 \end{bmatrix}.
\]
Thus, $\zeta_8^{-1}\alpha^3$ lies in $K_{(2)}$, so does $\alpha^4/\zeta_8^{-1}\alpha^3 = \zeta_8\alpha$. Lastly, since $\alpha^{12}$ generates $K_{(2)}$ over $K$, so does $\zeta_8\alpha$. Therefore, we are done.

(ii) Let $\alpha = g_{[1/2]}(\tau_K)$. Since $\gamma_2(\tau_K) = (\alpha^{12} + 16)/\alpha^4$ by Lemma 4.1(ii) and $\alpha^4 \in K_{(2)} \cap \mathbb{R}$ by (i), we have $\gamma_2(\tau_K) \in K_{(2)} \cap \mathbb{R}$. Note from Remark 4.7 that $g_{[1/2]}(\tau_K)^{12}$ and $g_{[1/2]}(\tau_K)^{12}$ are the two conjugates of $\alpha^{12}$ over $H_K$. In particular, $g_{[1/2]}(\tau_K)^{4}$ and $g_{[1/2]}(\tau_K)^{4}$ belong to $K_{(2)}$ by Lemma 4.1(iii). Hence, the other two conjugates of $\alpha^{4}$ over $H_K$ are $\xi_1 g_{[1/2]}(\tau_K)^{4}$ and $\xi_2 g_{[1/2]}(\tau_K)^{4}$ for some cube roots of unity $\xi_1, \xi_2$. If $\zeta_4$ lies in $K_{(2)}$, then $3$ ramifies in $K_{(2)}$ (but not in $K$ by hypothesis), which contradicts the fact that all prime ideals of $K$ which are ramified in $K_{(2)}$ must divide $(2)$. So we get $\xi_1 = \xi_2 = 1$. And, Lemma 4.1(ii) shows that $\gamma_2(\tau_K)$ is invariant under the action of $\text{Gal}(K_{(2)}/H_K)$; and hence $\gamma_2(\tau_K) \in H_K$. Therefore, we conclude that $\gamma_2(\tau_K)$ is a real algebraic integer which generates $H_K$ over $K$ by the fact $j(\tau_K) = \gamma_2(\tau_K)^3$ and Proposition 4.4(i). \hfill \Box

Remark 4.9. Observe that $\zeta_4 g_{[1/2]}(\tau_K) = \zeta_4 f_2(\tau_K)^2$ by (18). Besides Theorem 4.8 there are several other theorems which assert that the singular values of the Weber functions and $\gamma_2(\tau)$ generate class fields of imaginary quadratic fields ([27, §126–127], [19], [21], [4, §12]) whose proofs are quite classical. However, they are certainly elegant and worthy of considering. On the other hand, Gee [7] applied Shimura’s reciprocity law to the Weber functions which satisfy the following transformation properties:
\[
f(\tau) \circ T = \zeta_{48} f_1(\tau), \quad f_1(\tau) \circ T = \zeta_8^{-1} f(\tau), \quad f_2(\tau) \circ T = \zeta_{24} f_2(\tau),
\]
\[
f(\tau) \circ S = f(\tau), \quad f_1(\tau) \circ S = f_2(\tau), \quad f_2(\tau) \circ S = f_1(\tau),
\]
where $T = [\frac{1}{2} \, 1 \, 1]$ and $S = [\frac{1}{2} \, -1 \, 0]$ are the generators of $\text{SL}_2(\mathbb{Z})$. But, the general transformation formula for
\[
f(\tau) \circ \gamma \quad (f(\tau) = f(\tau), f_1(\tau), f_2(\tau), \gamma \in \text{SL}_2(\mathbb{Z}))
\]
does not seem to be known, which forces her to produce a redundant step to decompose $\gamma$ into a product of $T$ and $S$ [7, §5]. Thus we would like to point out that the relation (18) and Proposition 2.3(ii), (iii) will give us an explicit formula for $f(\tau)^2 \circ \gamma$, from which one can efficiently apply Shimura’s reciprocity law.
5. Application to class number one problem

In this section we shall revisit Gauss’ class number one problem for imaginary quadratic fields.

Let \( K \) be an imaginary quadratic field of discriminant \( d_K \). Since \( j(\tau_K) \) is a real algebraic integer lying in \( H_K \) by Proposition 4.4(i), it should be an integer when \( K \) has class number one. By determining the form class group \( C(d_K) \) we know that there are only nine imaginary quadratic fields \( K \) of class number one with \( d_K \geq -163 \) [4, p. 261]:

**Table 1.** Imaginary quadratic fields \( K \) of class number one with \( d_K \geq -163. \)

<table>
<thead>
<tr>
<th>( d_K )</th>
<th>( \mathbb{Q}(\sqrt{-3}) )</th>
<th>( \mathbb{Q}(\sqrt{-4}) )</th>
<th>( \mathbb{Q}(\sqrt{-7}) )</th>
<th>( \mathbb{Q}(\sqrt{-2}) )</th>
<th>( \mathbb{Q}(\sqrt{-11}) )</th>
<th>( \mathbb{Q}(\sqrt{-19}) )</th>
<th>( \mathbb{Q}(\sqrt{-43}) )</th>
<th>( \mathbb{Q}(\sqrt{-67}) )</th>
<th>( \mathbb{Q}(\sqrt{-163}) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( j(\tau_K) )</td>
<td>( 0 )</td>
<td>( 12^1 )</td>
<td>( -13^1 )</td>
<td>( 20^3 )</td>
<td>( -32^3 )</td>
<td>( -96^3 )</td>
<td>( -960^3 )</td>
<td>( -5280^3 )</td>
<td>( -640320^3 )</td>
</tr>
<tr>
<td>( \tau_0 )</td>
<td>( 0 )</td>
<td>( 12 )</td>
<td>( -15 )</td>
<td>( 20 )</td>
<td>( -32 )</td>
<td>( -96 )</td>
<td>( -960 )</td>
<td>( -5280 )</td>
<td>( -640320 )</td>
</tr>
</tbody>
</table>

We shall show in this section that the above table is the complete one by utilizing Shimura’s reciprocity law and Siegel functions.

**Lemma 5.1.** Let \( \tau_0 \in \mathbb{H} \), and set \( A = |e^{2\pi i \tau_0}|. \)

(i) If \([\frac{a}{b}] \in \mathbb{Q}^2 \) with \( 0 < a \leq 1/2 \), then \( |g_{[\frac{a}{b}]}(\tau_0)| \leq A^{(1/2)B_2(a)}e^{2A^a/(1-A)}. \)

(ii) If \( b \in \mathbb{Q} \) with \( 0 < b < 1 \), then \( |g_{[\frac{a}{b}]}(\tau_0)| \leq A^{(1/2)B_2(0)}|1-e^{2\pi ib}|e^{2A^a/(1-A)}. \)

**Proof.** (i) We derive from the definition (1) that

\[
|g_{[\frac{a}{b}]}(\tau_0)| \leq A^{(1/2)B_2(a)}(1 + A^a) \prod_{n=1}^{\infty} (1 + A^{n+a})(1 + A^{n-a})
\]

\[
\leq A^{(1/2)B_2(a)} \prod_{n=0}^{\infty} (1 + A^{n+a})^2 \quad \text{by the facts } A < 1 \text{ and } 0 < a \leq 1/2
\]

\[
\leq A^{(1/2)B_2(a)} \prod_{n=0}^{\infty} e^{2A^{n+a}} \quad \text{by the inequality } 1 + X < e^X \text{ for } X > 0
\]

\[
= A^{(1/2)B_2(a)}e^{2A^a/(1-A)}.
\]

(ii) In a similar way, we get that

\[
|g_{[\frac{b}{a}]}(\tau_0)| \leq A^{(1/2)B_2(0)}|1 - e^{2\pi ib}| \prod_{n=1}^{\infty} (1 + A^n)^2
\]

\[
\leq A^{(1/2)B_2(0)}|1 - e^{2\pi ib}| \prod_{n=1}^{\infty} e^{2A^n}
\]

by the inequality \( 1 + X < e^X \) for \( X > 0 \)

\[
= A^{(1/2)B_2(0)}|1 - e^{2\pi ib}|e^{2A^a/(1-A)}. \quad \square
\]
Theorem 5.2. Let \( K \neq \mathbb{Q}(\sqrt{-3}), \mathbb{Q}(\sqrt{-1}) \) be an imaginary quadratic field of discriminant \( d_K \). Assume that \( K \) has class number one (that is, \( H_K = K \)).

(i) If 2 is not inert in \( K \), then \( d_K = -7, -8 \).
(ii) If 2 is inert and 3 is ramified in \( K \), then there is no such \( K \).
(iii) If 2 is inert and 3 is not ramified in \( K \), then \( d_K = -11, -19, -43, -67, -163 \).

Proof. Since we are assuming that \( K \) is neither \( \mathbb{Q}(\sqrt{-3}) \) nor \( \mathbb{Q}(\sqrt{-1}) \), we have \( d_K \leq -7 \). Let \( \alpha = g_{\frac{1}{12}}(\tau_K) \neq 0 \) and \( A = e^{-\pi \sqrt{d_K}} \).

(i) If \( d_K \leq -31 \), then we see that

\[
|N_{K(3)/K}(\alpha^{12})|^{1/12} = \left\{ \begin{array}{ll}
|g_{\frac{1}{2}}(\tau_K)g_{\frac{1}{12}}(\tau_K)| & \text{if } d_K \equiv 0 \pmod{8}, \\
|g_{\frac{1}{2}}(\tau_K)g_{\frac{1}{2}}(\tau_K)| & \text{if } d_K \equiv 4 \pmod{8}, \\
|g_{\frac{1}{2}}(\tau_K)| & \text{if } d_K \equiv 1 \pmod{8},
\end{array} \right.
\]

\[
\leq \left\{ \begin{array}{ll}
2A^{1/12}e^{2A/(1-A)} \cdot A^{-1/24}e^{2A^{1/2}/(1-A)} & \text{if } d_K \equiv 0 \pmod{4}, \\
2A^{1/12}e^{2A/(1-A)} & \text{if } d_K \equiv 1 \pmod{8},
\end{array} \right.
\]

\[
< 1 \quad \text{by the fact } A \leq e^{-\pi \sqrt{d}}.
\]

On the other hand, since \( N_{K(3)/K}(\alpha^{12}) \) is a nonzero integer by Theorem 4.6(ii), the above inequality is false; hence \( d_K > -31 \). And, we get the conclusion by Table 1.

(ii) Since 2 is inert and 3 is ramified in \( K \) (equivalently, \( d_K \equiv 21 \pmod{24} \)), we have

\[
\text{Gal}(K(3)/K) \simeq W_{3,\tau_K}/\text{Ker}_{3,\tau_K} = \left\{ \begin{array}{ccc}
1 & 0 \\
0 & 1
\end{array} \right\}, \left\{ \begin{array}{ccc}
1 & 0 \\
2 & 1
\end{array} \right\}
\]

by Proposition 2.5. Let \( \beta = g_{\frac{1}{1/3}}(\tau_K) \neq 0 \). Since \( g_{\frac{1}{1/3}}(\tau) \) \( \in \mathfrak{F}_3 \) by Proposition 2.1, we have \( \beta^{12} \in K_{(3)} \) by Proposition 2.4. Furthermore, since \( \beta^{12} \) is a real algebraic integer by the definition (1), Propositions 2.3(vi) and 4.4(i), \( N_{K(3)/K}(\beta^{12}) \) is a nonzero integer by Lemma 4.3. If \( d_K \leq -51 \), then we derive that

\[
|N_{K(3)/K}(\beta^{12})|^{1/12} = \left| g_{\frac{1}{1/3}}(\tau_K)g_{\frac{1}{1/3}}(\tau_K)g_{\frac{1}{2/3}}(\tau_K) \right| \quad \text{by Proposition 2.3(iv) and (v)}
\]

\[
\leq A^{1/12}|1 - \zeta_3 e^{2A/(1-A)}| \cdot (A^{-1/30}e^{2A^{1/2}/(1-A)})^2 \quad \text{by Lemma 5.1}
\]

\[
= \sqrt{3}A^{1/30}e^{2A+4A^{1/2}/(1-A)}.
\]

\[
< 1 \quad \text{by the fact } A \leq e^{-\pi \sqrt{d}}.
\]
Hence we must have $-51 < d_K \leq -7$. But there is no such imaginary quadratic field $K$ with $d_K \equiv 21 \pmod{24}$ as desired.

(iii) Let $x = \zeta_8 \alpha$. Since $[K(2) : K] = 3$ by the degree formula (15), we have

\[ \min(x, K) = X^3 + aX^2 + bX + c \quad \text{for some } a, b, c \in \mathbb{Z} \]

by Theorem 4.8(i) and Lemma 4.3. Furthermore, we get

\[ \min(x^4, K) = X^3 - \gamma_2(\tau_K)X - 16 \quad (\in \mathbb{Z}[X]) \]

by Lemma 4.1(ii) and Theorem 4.8(ii). Now, by adopting Heegner’s idea [9] one can determine the possible values of $a, b, c$, from which we obtain

\[ \gamma_2(\tau_K) = 0, -32, -96, -960, -5280, -640320. \]

Therefore, we can conclude the assertion (iii) by Table 1 and Lemma 3.2, although we omit the details [4, pp. 272–274]. \qed

Remark 5.3. (i) In 1903 Landau ([13] or [4, Theorem 2.18]) presented a simple and elementary proof of Theorem 5.2(i) by considering the form class group $C(d_K)$.

(ii) Theorem 4.8(i) is essentially a gap in Heegner’s work, which was fulfilled by Stark [25].

(iii) To every imaginary quadratic order $\mathcal{O}$ of class number one there is an associated elliptic curve $E_{\mathcal{O}}$ over $\overline{\mathbb{Q}}$ admitting complex multiplication by $\mathcal{O}$. It can be defined over $\mathbb{Q}$ and is unique up to $\overline{\mathbb{Q}}$-isomorphism. For a positive integer $n$, let $X^+_n(n)$ be the modular curve associated to the normalizer of the non-split Cartan subgroup of level $n$ which can be defined over $\mathbb{Q}$ [3]. If every prime $p$ dividing $n$ is inert in $\mathcal{O}$, then $E_{\mathcal{O}}$ gives rise to an integral point of $X^+_n(n)$ [22, p. 195]. Here, by integral points we mean the points corresponding to elliptic curves with integral $j$-invariant. As Serre pointed out [22, p. 197], the solutions by Heegner and Stark can be viewed as the determination of the integral points of $X^+_n(24)$. And, Baran [2] recently gave a geometric solution of the class number one problem by finding an explicit parametrization for the modular curve $X^+_n(9)$ over $\mathbb{Q}$.

We can also apply the arguments in the proof of Theorem 5.2(i) and (ii) to solve a problem concerning imaginary quadratic fields of class number two.

**Theorem 5.4.** $\mathbb{Q}(\sqrt{-15})$ is the unique imaginary quadratic field of class number two in which 2 splits.

**Proof.** Let $K$ be an imaginary quadratic field of discriminant $d_K$ and class number two in which 2 splits (so $d_K \equiv 1 \pmod{8}$). Then the form class group $C(d_K)$ consists of two reduced quadratic forms, that is

\[ Q_1 = X^2 + XY + ((1 - d_K)/4)Y^2; \]
\[ Q_2 = aX^2 + bXY + cY^2 \quad \text{for some } a, b, c \in \mathbb{Z} \text{ with } 2 \leq a \leq \sqrt{|d_K|}/3. \]
And, we have by Proposition 2.6 with \( p = 2 \)
\[
\tau_{Q_1} = (-1 + \sqrt{d_K})/2, \quad u_{Q_1} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix},
\]
\[
\tau_{Q_2} = (b + \sqrt{d_K})/2a, \quad u_{Q_2} = \begin{bmatrix} * & * \\ r & s \end{bmatrix}
\text{ for some } \begin{bmatrix} r \\ s \end{bmatrix} \in \{ \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \end{bmatrix} \).
\]
Let \( \alpha = g_{[1/2]}(\tau_K) \) \((\neq 0)\). Then \( \alpha^{12} \in H_K \) by (19). If \( d_K \leq -31 \), then we derive that
\[
|N_{H_K/K}(\alpha^{12})|^{1/12} = \prod_{Q \in \mathcal{C}(d_K)} |g_{[1/2]}(\tau)^{12}u_0(\tau_Q)|^{1/12}
\text{ by Proposition 2.6}
\]
\[
= |g_{[1/2]}(\tau)^{(1 + \sqrt{d_K})/2})| \times |g_{[r/2]}((b + \sqrt{d_K})/2a)|
\text{ by Proposition 2.3(iv) and (v)}
\]
\[
\leq 2A^{1/12}e^{2A/(1-A)} \times \begin{cases} 
2A^{1/12}e^{2A/(1-A)} & \text{if } r = 0,
A^{-1/24}e^{2A/(1-A)} & \text{if } r = 1
\end{cases}
\text{ with } A = e^{-\pi \sqrt{|d_K|}} \text{ by Lemma 5.1}
\]
\[
\leq \begin{cases} 
4A^{1/12}e^{2A/(1-A)}-\pi^{1/12}+2e^{-\pi \sqrt{2}}/(1-e^{-\pi \sqrt{2}}) & \text{if } r = 0,
2A^{1/12}e^{2A/(1-A)}+2e^{-\pi \sqrt{2}}/(1-e^{-\pi \sqrt{2}}) & \text{if } r = 1
\end{cases}
\text{ because } A < 1 \text{ and } 2 \leq a \leq \sqrt{|d_K|/3}
< 1 \text{ by the fact } A \leq e^{-\pi \sqrt{31}}.
\]
On the other hand, since \( \alpha^{12} \) is a real algebraic integer, \( N_{H_K/K}(\alpha^{12}) \) is a nonzero integer by Lemma 4.3. Therefore we should have \( d_K > -31 \). One can then easily see by the following remark that \( \mathbb{Q}(\sqrt{-15}) \) is the unique one. \( \square \)

\textbf{Remark 5.5.} There are exactly eighteen imaginary quadratic fields of class number two whose discriminants are as follows [18, p. 636]:
\[
-15, -20, -24, -35, -40, -51, -52, -88, -91, -115,
\]

\textbf{References}


Department of Mathematics
Hankuk University of Foreign Studies
Yongin 449-791, Korea
E-mail address: dshin@hufs.ac.kr