NORMAL BASES OF THE RAY CLASS FIELDS OVER IMAGINARY QUADRATIC FIELDS

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

Abstract. We develop a criterion for determining normal bases, and by making use of necessary lemmas refined a little from [3] we further prove that the singular values of certain Siegel functions form normal bases of the ray class fields over all imaginary quadratic fields other than $\mathbb{Q}(\sqrt{-1})$ and $\mathbb{Q}(\sqrt{-3})$.

1. Introduction

Let L be a finite Galois extension of a field K. Then from the normal basis theorem([14]) we know that there exists a normal basis of L over K, namely a basis of the form $\{x^\gamma : \gamma \in \mathrm{Gal}(L/K)\}$ for a single element $x \in L$.

Okada([9]) showed that if $k \geq 1$ and $q > 2$ are integers such that $k \equiv 1 \pmod 2$ and T is a set of representatives for which $(\mathbb{Z}/q\mathbb{Z})^\times = T \cup (-T)$, then the real numbers $\left(\frac{1}{\pi}\frac{d}{dz}\right)^k(\cot \pi z)|_{z=\frac{a}{q}}$ for $a \in T$ form a normal basis of the maximal real subfield of $\mathbb{Q}(e^{\frac{2\pi i}{q}})$ over $\mathbb{Q}$. Replacing the cotangent function by the Weierstrass $\wp$-function with fundamental period i and 1, he further obtained normal bases of the class fields over the Gauss' number field $\mathbb{Q}(\sqrt{-1})$([10]). This result was due to the fact that the Gauss's number field has class number 1, which can be naturally extended to any imaginary quadratic field with class number 1.

After Okada, Taylor([13]) and Schertz([11]) established the Galois module structures of the rings of integers of certain abelian extensions over an imaginary quadratic field, which are analogues of the cyclotomic case([8]). They also found normal bases by the special values of modular functions. And, Komatsu([4]) considered certain abelian extensions L and K of $\mathbb{Q}(e^{\frac{2\pi i}{5}})$ and constructed a normal basis of L over K by the special values of Siegel modular functions.

In this paper we shall present normal bases of the ray class fields over all imaginary quadratic fields($\neq \mathbb{Q}(\sqrt{-1}),\ \mathbb{Q}(\sqrt{-3})$) in terms of the singular values of certain Siegel functions(Theorem 4.5 and Remark 4.6) by applying a criterion for determining normal bases which will be developed in section 2.

For any pair $(r_1, r_2) \in \mathbb{Q}^2 \setminus \mathbb{Z}^2$ we define a Siegel function $g_{(r_1,r_2)}(\tau)$ on $\mathfrak{H}$(the complex upper half plane) by the following Fourier expansion

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

where $\mathbf{B}_2(X) = X^2 - X + \frac{1}{6}$ 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 [6].

2000 *Mathematics Subject Classification.* 11F11, 11F20, 11R37, 11Y40.

Key words and phrases. modular forms and functions, class fields, normal bases.

This work was supported by the SRC Program of KOSEF Research Grant R11-2007-035-01001-0.

Let $K \neq \mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-3})$ be an imaginary quadratic field of discriminant d_K and $\mathcal{O}_K = \mathbb{Z}[\theta]$ be the ring of integers with

$$\theta = \begin{cases} \frac{\sqrt{d_K}}{2} & \text{for} \quad d_K \equiv 0 \pmod 4 \\ \frac{-1+\sqrt{d_K}}{2} & \text{for} \quad d_K \equiv 1 \pmod 4). \end{cases}$$

In what follows we denote the Hilbert class field and the ray class field modulo N of K for an integer $N \geq 2$ by H and $K_{(N)}$, respectively. In [3] we showed that the value $x = g_{(0,\frac{1}{N})}^{\frac{-12N}{\gcd(6,N)}}(\theta)$ is a primitive generator of $K_{(N)}$ over K except possibly finitely many cases. We achieved this result by showing that the absolute value of x is the smallest one among all its conjugates.

In this article we will prove that the conjugates of a high power of x form a normal basis of $K_{(N)}$ over K by applying Lemma 4.2∼4.4 originally investigated in [3]. On the other hand, we shall manipulate the action of $\mathrm{Gal}(K_{(N)}/K)$ on x by following Gee's idea([2]) which will be summarized in section 3.

2. A criterion for determining normal bases

In this section let L be a finite abelian extension of a number field K with $G = \mathrm{Gal}(L/K) = \{\gamma_1 = \mathrm{id}, \cdots, \gamma_n\}$. Further we let $|\cdot|$ be the usual absolute value defined on $\mathbb{C}$.

Lemma 2.1. *A set of elements $\{x_1, \cdots, x_n\}$ in L is a K-basis of L if and only if*

$$\det_{1\leq i,j\leq n}\left(x_i^{\gamma_j^{-1}}\right) \neq 0.$$

Proof. Straightforward. □

By $\widehat{G}$ we denote the character group of G. Then we have the *Frobenius determinant relation*:

Lemma 2.2. *If f is any $\mathbb{C}$-valued function on G, then*

$$\prod_{\chi\in\widehat{G}}\sum_{1\leq i\leq n}\chi(\gamma_i^{-1})f(\gamma_i) = \det_{1\leq i,j\leq n}\left(f(\gamma_i\gamma_j^{-1})\right).$$

Proof. See [7] Chapter 21 Theorem 5. □

Combining Lemma 2.1 and Lemma 2.2 we derive the following proposition:

Proposition 2.3. *The conjugates of an element $x \in L$ form a normal basis of L over K if and only if*

$$\sum_{1\leq i\leq n}\chi(\gamma_i^{-1})x^{\gamma_i} \neq 0 \textit{ for all } \chi \in \widehat{G}.$$

Proof. For an element $x \in L$, set $x_i = x^{\gamma_i}$ for $1 \leq i \leq n$. Then we get that

$$\begin{aligned} & \text{the conjugates of } x \text{ form a normal basis of } L \text{ over } K \\ \Longleftrightarrow\ & \{x_1, \cdots, x_n\} \text{ is a } K\text{-basis of } L \text{ by the definition of a normal basis} \\ \Longleftrightarrow\ & \det_{1\leq i,j\leq n}\left(x_i^{\gamma_j^{-1}}\right) \neq 0 \text{ by Lemma 2.1} \\ \Longleftrightarrow\ & \sum_{1\leq i\leq n}\chi(\gamma_i^{-1})x_i \neq 0 \text{ for all } \chi \in \widehat{G} \text{ by Lemma 2.2 with } f(\gamma_i) = x_i. \end{aligned}$$

□

Now we present a simple criterion which enables us to determine whether the conjugates of an element $x \in L$ form a normal basis of L over K.

Theorem 2.4. *Assume that there exists an element $x \in L$ such that*

$$\left|\frac{x^{\gamma_i}}{x}\right| < 1 \text{ for } 1 < i \leq n. \tag{2.1}$$

Then the conjugates of a high power of x form a normal basis of L over K.

Proof. By the hypothesis (2.1) we can take a suitably large integer m such that

$$\left|\frac{x^{\gamma_i}}{x}\right|^m \leq \frac{1}{\#G} \text{ for } 1 < i \leq n \tag{2.2}$$

where $\#G$ is the cardinality of G. Then for $\chi \in \widehat{G}$ we have

$$\begin{aligned}\left|\sum_{1\leq i\leq n} \chi(\gamma_i^{-1})(x^m)^{\gamma_i}\right| &\geq |x^m|\left(1 - \sum_{1<i\leq n}\left|\frac{(x^m)^{\gamma_i}}{x^m}\right|\right) \text{ by the triangle inequality}\\ &\geq |x^m|\left(1 - \frac{1}{\#G}(\#G-1)\right) = \frac{|x^m|}{\#G} > 0 \text{ by (2.2).}\end{aligned}$$

Therefore the conjugates of x^m form a normal basis of L over K by Proposition 2.3. □

3. Action of Galois groups

We shall investigate an algorithm for finding all conjugates of the singular value of a modular function, from which we can determine the conjugates of the singular values of certain Siegel functions due to [2] and [3].

For a positive integer N let $\mathcal{F}_N$ be the field of modular functions of level N defined over N-th cyclotomic field over $\mathbb{Q}$. Then $\mathcal{F}_N$ is a Galois extension of $\mathcal{F}_1 = \mathbb{Q}(j)$($j$ =the elliptic modular function) and its Galois group is isomorphic to $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1_2\}$([12], [7]).

Throughout this section we let $K \neq \mathbb{Q}(\sqrt{-1}),\ \mathbb{Q}(\sqrt{-3})$ be an imaginary quadratic field with discriminant d_K and define

$$\theta = \begin{cases} \frac{\sqrt{d_K}}{2} & \text{for} \quad d_K \equiv 0 \pmod 4 \\ \frac{-1+\sqrt{d_K}}{2} & \text{for} \quad d_K \equiv 1 \pmod 4. \end{cases} \tag{3.1}$$

Under the properly equivalent relation, primitve definite quadratic forms $aX^2 + bXY + cY^2$ of discriminant d_K determine a group $C(d_K)$, called the *form class group of discriminant d_K*. We identify $C(d_K)$ with the set of all *reduced quadratic forms*, which are characterized by the conditions

$$-a < b \leq a < c \quad \text{or} \quad 0 \leq b \leq a = c \tag{3.2}$$

together with the discriminant relation

$$b^2 - 4ac = d_K. \tag{3.3}$$

From the above two conditions for reduced quadratic forms we have

$$1 \leq a \leq \sqrt{\tfrac{-d_K}{3}}. \tag{3.4}$$

Then it is well-known that $C(d_K)$ is isomorphic to $\mathrm{Gal}(H/K)$([1]). For a reduced form $Q = aX^2 + bXY + cY^2$ of discriminant d_K we define

$$\theta_Q = \frac{-b + \sqrt{d_K}}{2a}. \tag{3.5}$$

Furthermore, we define $\beta_Q=(\beta_p)_p\in\prod_{p\,:\,\mathrm{prime}}\mathrm{GL}_2(\mathbb{Z}_p)$ as

$$(3.6)\qquad \beta_p=\begin{cases}\begin{pmatrix}a&\frac{b}{2}\\0&1\end{pmatrix} & \text{if}\quad p\nmid a\\ \begin{pmatrix}-\frac{b}{2}&-c\\1&0\end{pmatrix} & \text{if}\quad p\mid a\quad\text{and}\quad p\nmid c\\ \begin{pmatrix}-\frac{b}{2}-a&-\frac{b}{2}-c\\1&-1\end{pmatrix} & \text{if}\quad p\mid a\quad\text{and}\quad p\mid c\end{cases}\qquad \text{for } d_K\equiv 0\pmod 4$$

and

$$(3.7)\quad \beta_p=\begin{cases}\begin{pmatrix}a&\frac{b-1}{2}\\0&1\end{pmatrix} & \text{if}\quad p\nmid a\\ \begin{pmatrix}\frac{-b-1}{2}&-c\\1&0\end{pmatrix} & \text{if}\quad p\mid a\quad\text{and}\quad p\nmid c\\ \begin{pmatrix}\frac{-b-1}{2}-a&\frac{1-b}{2}-c\\1&-1\end{pmatrix} & \text{if}\quad p\mid a\quad\text{and}\quad p\mid c\end{cases}\qquad \text{for } d_K\equiv 1\pmod 4).$$

Let $\mathrm{irr}(\theta,K)=X^2+BX+C\in\mathbb{Z}[X]$ and $N\geq 2$. Considering the group

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

we have an isomorphism $\mathrm{Gal}(K_{(N)}/H)\cong W_{N,\theta}/\{\pm 1_2\}$([2]).

Proposition 3.1. *Let $K\neq\mathbb{Q}(\sqrt{-1}),\ \mathbb{Q}(\sqrt{-3})$ be an imaginary quadratic field and $N\geq 2$. Then we have an isomorphism*

$$\begin{array}{ccc}W_{N,\theta}/\{\pm 1_2\}\cdot C(d_K) & \longrightarrow & Gal(K_{(N)}/K)\\ \alpha\cdot Q & \longmapsto & \big(h(\theta)\mapsto h^{\alpha\cdot\beta_Q}(\theta_Q)\big).\end{array}$$

Here $h\in\mathcal{F}_N$ is defined and finite at θ, and θ, θ_Q are defined as in (3.1) and (3.5), respectively. The action of α on $\mathcal{F}_N$ is the action as an element of $GL_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1_2\}\cong Gal(\mathcal{F}_N/\mathcal{F}_1)$. As for β_Q we note that there exists $\beta\in GL_2^+(\mathbb{Q})\cap M_2(\mathbb{Z})$ such that $\beta\equiv\beta_p\pmod{N\mathbb{Z}_p}$ for all primes p dividing N by the Chinese remainder theorem. Then the action of β_Q on $\mathcal{F}_N$ is understood as that of β which is an element of $GL_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1_2\}$([12] *or* [2]*).*

Proof. See [3] Theorem 3.4. □

Proposition 3.1 and the transformation formulas of Siegel functions in the next proposition enable us to find all conjugates of the singular value $g_{(0,\frac{1}{N})}^{\frac{-12N}{\gcd(6,N)}}(\theta)$, which will be used to prove our main theorem.

Proposition 3.2. *Let $N\geq 2$. For $(v,w)\in\mathbb{Z}^2\setminus N\mathbb{Z}^2$ the function $g_{(\frac{v}{N},\frac{w}{N})}^{\frac{-12N}{\gcd(6,N)}}(\tau)$ satisfies*

$$g_{(\frac{v}{N},\frac{w}{N})}^{\frac{-12N}{\gcd(6,N)}}(\tau)=g_{(\frac{-v}{N},\frac{-w}{N})}^{\frac{-12N}{\gcd(6,N)}}(\tau)=g_{(\langle\frac{v}{N}\rangle,\langle\frac{w}{N}\rangle)}^{\frac{-12N}{\gcd(6,N)}}(\tau)$$

where $\langle X\rangle$ is the fractional part of $X\in\mathbb{R}$ such that $0\leq\langle X\rangle<1$. It belongs to $\mathcal{F}_N$ and α in $GL_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1_2\}\cong Gal(\mathcal{F}_N/\mathcal{F}_1)$ acts on the function by

$$\big(g_{(\frac{v}{N},\frac{w}{N})}^{\frac{-12N}{\gcd(6,N)}}(\tau)\big)^{\alpha}=g_{(\frac{v}{N},\frac{w}{N})\alpha}^{\frac{-12N}{\gcd(6,N)}}(\tau).$$

Proof. See [5] Proposition 2.4 and Theorem 2.5. □

4. Normal bases of $K_{(N)}$ over K

Let $K \neq \mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-3})$ be an imaginary quadratic field so that $d_K \leq -7$, and let θ be defined as in (3.1) and $N \geq 2$ be an integer. If we put

$$D = \sqrt{\tfrac{-d_K}{3}} \quad \text{and} \quad A = |e^{2\pi i\theta}| = e^{-\pi\sqrt{-d_K}},$$

then $A^{\frac{1}{D}} = e^{-\sqrt{3}\pi}$, which is independent of K.

Lemma 4.1. *We have the following inequalities:*

(i) $1 < \left|\frac{1-\zeta_N}{1-A^{\frac{1}{DN}}}\right| < A'(N)$ *where* $A'(N) = \begin{cases} 2.141 & \textit{if } N = 2,\ 3 \\ 1.903 & \textit{if } N = 4 \\ 1.773 & \textit{if } N = 5 \\ 1.678 & \textit{if } N = 6 \\ 1.606 & \textit{if } N = 7,\ 8 \\ 1.508 & \textit{if } N = 9,\ 10,\ 11 \\ 1.42 & \textit{if } N = 12, \cdots, 17 \\ 1.332 & \textit{if } N = 18,\ 19,\ 20 \\ 1.306 & \textit{if } N \geq 21. \end{cases}$

(ii) If $N \geq 2$, *then* $\left|\frac{1-\zeta_N}{1-\zeta_N^t}\right| \leq 1$ *for all* $t \in \mathbb{Z} \setminus N\mathbb{Z}$.

(iii) If $N \geq 4$, *then* $\left|\frac{1-\zeta_N}{1-\zeta_N^t}\right| \leq \frac{1}{\sqrt{2}}$ *for* $2 \leq t \leq \frac{N}{2}$.

(iv) If $N \geq 2$, *then* $A^{\frac{1}{2}(\mathbf{B}_2(0)-\mathbf{B}_2(\frac{1}{N}))}\left|\frac{1-\zeta_N}{1-A^{\frac{1}{N}}}\right| < 0.76$.

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

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

(vii) $1 + X < e^X$ *for all* $X > 0$.

Proof. See [3] Lemma 4.1. □

Although the following lemmas are given in [3], we present the proofs for the sake of completeness.

Lemma 4.2. *Assume the condition*

$$\begin{cases} d_K \leq -11, & N = 2,\ 3 \\ d_K \leq -8, & N = 4 \\ d_K \leq -31, & N = 5 \\ d_K \leq -23, & N = 6 \\ d_K \leq -19, & N = 7,\ 8 \\ d_K \leq -15, & N = 9,\ 10,\ 11 \\ d_K \leq -11, & N = 12, \cdots, 17 \\ d_K \leq -8, & N = 18,\ 19,\ 20 \\ d_K \leq -7, & N \geq 21. \end{cases} \tag{4.1}$$

Let $Q = aX^2 + bXY + cY^2$ *be a reduced quadratic form of discriminant* d_K. *If* $a \geq 2$, *then the inequality*

$$\left|\frac{g^{-1}_{(\frac{s}{N},\frac{t}{N})}(\theta_Q)}{g^{-1}_{(0,\frac{1}{N})}(\theta)}\right| < 1$$

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

Proof. We may assume $0 \leq s \leq \frac{N}{2}$ by Proposition 3.2. And, note that $2 \leq a \leq D$ by (3.4). From the definition (1.1) we obtain that

$$\left|\frac{g^{-1}_{(\frac{s}{N},\frac{t}{N})}(\theta_Q)}{g^{-1}_{(0,\frac{1}{N})}(\theta)}\right| \leq A^{\frac{1}{2}(\mathbf{B}_2(0)-\frac{1}{a}\mathbf{B}_2(\frac{s}{N}))}\left|\frac{1-\zeta_N}{1-e^{2\pi i(\frac{s}{N}\cdot\frac{-b+\sqrt{d_K}}{2a}+\frac{t}{N})}}\right|\prod_{n=1}^{\infty}\frac{(1+A^n)^2}{(1-A^{\frac{1}{a}(n+\frac{s}{N})})(1-A^{\frac{1}{a}(n-\frac{s}{N})})}.$$

If $s = 0$, then we get by Lemma 4.1(ii)

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

If $s \neq 0$, then by the fact $2 \leq a \leq D$ and Lemma 4.1(i) we derive

$$\left|\frac{1-\zeta_N}{1-e^{2\pi i(\frac{s}{N}\cdot\frac{-b+\sqrt{d_K}}{2a}+\frac{t}{N})}}\right| \leq \left|\frac{1-\zeta_N}{1-A^{\frac{s}{Na}}}\right| \leq \left|\frac{1-\zeta_N}{1-A^{\frac{1}{ND}}}\right| < A'(N).$$

Let

$$A'(s,N) = \begin{cases} 1 & \text{if } s = 0 \\ A'(N) & \text{if } s \neq 0. \end{cases}$$

On the other hand, by the facts $\mathbf{B}_2(\frac{1}{2}), \mathbf{B}_2(\frac{1}{3}), \mathbf{B}_2(\frac{1}{4}) < 0$ and $A < 1$ together with the assumption $a \geq 2$ we have

$$A^{\frac{1}{2}(\mathbf{B}_2(0)-\frac{1}{a}\mathbf{B}_2(\frac{s}{N}))} \leq A^{\varepsilon(s,N)} \text{ where } \varepsilon(s,N) = \begin{cases} \frac{1}{2}(\mathbf{B}_2(0)-\frac{1}{2}\mathbf{B}_2(0)) = \frac{1}{24} & \text{if } s = 0 \text{ or } N \geq 5 \\ \frac{1}{2}\mathbf{B}_2(0) = \frac{1}{12} & \text{otherwise.} \end{cases}$$

Therefore we achieve that

$$\begin{aligned}
\left|\frac{g^{-1}_{(\frac{s}{N},\frac{t}{N})}(\theta_Q)}{g^{-1}_{(0,\frac{1}{N})}(\theta)}\right| &\leq A^{\varepsilon(s,N)}A'(s,N)\prod_{n=1}^{\infty}\frac{(1+A^n)^2}{(1-A^{\frac{n}{D}})(1-A^{\frac{1}{D}(n-\frac{1}{2})})} \quad \text{by the facts } 2 \leq a \leq D,\ 0 \leq s \leq \tfrac{N}{2} \\
&< A^{\varepsilon(s,N)}A'(s,N)\prod_{n=1}^{\infty}(1+A^n)^2(1+A^{\frac{n}{1.03D}})(1+A^{\frac{1}{1.03D}(n-\frac{1}{2})}) \quad \text{by Lemma 4.1(v)} \\
&< A^{\varepsilon(s,N)}A'(s,N)\prod_{n=1}^{\infty}e^{2A^n+A^{\frac{n}{1.03D}}+A^{\frac{1}{1.03D}(n-\frac{1}{2})}} \quad \text{by Lemma 4.1(vii)} \\
&= A^{\varepsilon(s,N)}A'(s,N)e^{\frac{2A}{1-A}+\frac{A^{\frac{1}{1.03D}}+A^{\frac{1}{2.06D}}}{1-A^{\frac{1}{1.03D}}}} \\
&= \begin{cases}
e^{-\frac{\pi\sqrt{-d_K}}{24}}\ e^{\frac{2e^{-\pi\sqrt{-d_K}}}{1-e^{-\pi\sqrt{-d_K}}}+\frac{e^{-\frac{\sqrt{3}\pi}{1.03}}+e^{-\frac{\sqrt{3}\pi}{2.06}}}{1-e^{-\frac{\sqrt{3}\pi}{1.03}}}} & \text{if } s = 0 \\
e^{-\frac{\pi\sqrt{-d_K}}{24}}A'(N)\ e^{\frac{2e^{-\pi\sqrt{-d_K}}}{1-e^{-\pi\sqrt{-d_K}}}+\frac{e^{-\frac{\sqrt{3}\pi}{1.03}}+e^{-\frac{\sqrt{3}\pi}{2.06}}}{1-e^{-\frac{\sqrt{3}\pi}{1.03}}}} & \text{if } s \neq 0 \text{ and } N \geq 5 \\
e^{-\frac{\pi\sqrt{-d_K}}{12}}A'(N)\ e^{\frac{2e^{-\pi\sqrt{-d_K}}}{1-e^{-\pi\sqrt{-d_K}}}+\frac{e^{-\frac{\sqrt{3}\pi}{1.03}}+e^{-\frac{\sqrt{3}\pi}{2.06}}}{1-e^{-\frac{\sqrt{3}\pi}{1.03}}}} & \text{if } s \neq 0 \text{ and } N \leq 4
\end{cases} \\
&< 1 \quad \text{under the condition (4.1).}
\end{aligned}$$

This proves the lemma. □

Lemma 4.3. *Assume that $d_K \leq -7$ and $N \geq 2$. Let $Q = X^2 + bXY + cY^2$ be a reduced quadratic form of discriminant d_K. Then we have the inequality*

$$\left| \frac{g^{-1}_{(\frac{s}{N}, \frac{t}{N})}(\theta_Q)}{g^{-1}_{(0, \frac{1}{N})}(\theta)} \right| < 1$$

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

Proof. We may assume $1 \leq s \leq \frac{N}{2}$ by Proposition 3.2. Then we establish that

$$\begin{aligned}
\left| \frac{g^{-1}_{(\frac{s}{N}, \frac{t}{N})}(\theta_Q)}{g^{-1}_{(0, \frac{1}{N})}(\theta)} \right| &< A^{\frac{1}{2}(\mathbf{B}_2(0) - \mathbf{B}_2(\frac{s}{N}))} \left| \frac{1 - \zeta_N}{1 - A^{\frac{s}{N}}} \right| \prod_{n=1}^{\infty} \frac{(1 + A^n)^2}{(1 - A^{n + \frac{s}{N}})(1 - A^{n - \frac{s}{N}})} \quad \text{by (1.1)} \\
&< A^{\frac{1}{2}(\mathbf{B}_2(0) - \mathbf{B}_2(\frac{1}{N}))} \left| \frac{1 - \zeta_N}{1 - A^{\frac{1}{N}}} \right| \prod_{n=1}^{\infty} \frac{(1 + A^n)^2}{(1 - A^n)(1 - A^{n - \frac{1}{2}})} \quad \text{by the fact } 1 \leq s \leq \tfrac{N}{2} \\
&< 0.76 \prod_{n=1}^{\infty} (1 + A^n)^2 (1 + A^{\frac{n}{1.03}})(1 + A^{\frac{1}{1.03}(n - \frac{1}{2})}) \quad \text{by Lemma 4.1(iv) and (vi)} \\
&< 0.76 \prod_{n=1}^{\infty} e^{2A^n + A^{\frac{n}{1.03}} + A^{\frac{1}{1.03}(n - \frac{1}{2})}} = 0.76 e^{\frac{2A}{1-A} + \frac{A^{\frac{1}{1.03}} + A^{\frac{1}{2.06}}}{1 - A^{\frac{1}{1.03}}}} \quad \text{by Lemma 4.1(vii)} \\
&\leq 0.76 e^{\frac{2e^{-\sqrt{7}\pi}}{1 - e^{-\sqrt{7}\pi}} + \frac{e^{-\frac{\sqrt{7}\pi}{1.03}} + e^{-\frac{\sqrt{7}\pi}{2.06}}}{1 - e^{-\frac{\sqrt{7}\pi}{1.03}}}} < 1 \quad \text{by the fact } d_K \leq -7.
\end{aligned}$$

□

Lemma 4.4. *Assume the same condition as in Lemma 4.3 and let $Q = X^2 + bXY + cY^2$ be a reduced quadratic form of discriminant d_K. Then we deduce*

$$\left| \frac{g^{-1}_{(0, \frac{t}{N})}(\theta_Q)}{g^{-1}_{(0, \frac{1}{N})}(\theta)} \right| < 1$$

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

Proof. If $N = 2$ or 3, there is nothing to prove. Thus, let $N \geq 4$. Here we may assume $2 \leq t \leq \frac{N}{2}$ by Proposition 3.2. Then we get that

$$\begin{aligned}
\left| \frac{g^{-1}_{(0, \frac{t}{N})}(\theta_Q)}{g^{-1}_{(0, \frac{1}{N})}(\theta)} \right| &\leq \left| \frac{1 - \zeta_N}{1 - \zeta_N^t} \right| \prod_{n=1}^{\infty} \frac{(1 + A^n)^2}{(1 - A^n)^2} \\
&< \tfrac{1}{\sqrt{2}} \prod_{n=1}^{\infty} (1 + A^n)^2 (1 + A^{\frac{n}{1.03}})^2 \quad \text{by Lemma 4.1 (iii) and (vi)} \\
&< \tfrac{1}{\sqrt{2}} \prod_{n=1}^{\infty} e^{2A^n + 2A^{\frac{n}{1.03}}} \quad \text{by Lemma 4.1(vii)} \\
&= \tfrac{1}{\sqrt{2}} e^{\frac{2A}{1-A} + \frac{2A^{\frac{1}{1.03}}}{1 - A^{\frac{1}{1.03}}}} \leq \tfrac{1}{\sqrt{2}} e^{\frac{2e^{-\sqrt{7}\pi}}{1 - e^{-\sqrt{7}\pi}} + \frac{2e^{-\frac{\sqrt{7}\pi}{1.03}}}{1 - e^{-\frac{\sqrt{7}\pi}{1.03}}}} < 1 \quad \text{by the fact } d_K \leq -7,
\end{aligned}$$

which proves the lemma. □

Now we are ready to prove our main theorem concerning normal bases of $K_{(N)}$ over almost all K.

Theorem 4.5. *Assume the condition (4.1). Then for a suitably large integer m the conjugates of the value*

$$g_{(0,\frac{1}{N})}^{\frac{-12Nm}{\gcd(6,N)}}(\theta)$$

form a normal basis of $K_{(N)}$ over K.

Proof. For simplicity we put $x = g_{(0,\frac{1}{N})}^{\frac{-12N}{\gcd(6,N)}}(\theta)$, which belongs to $K_{(N)}$ by Proposition 3.2 and the main theorem of complex multiplication([12], [7]). Then it suffices to show by Theorem 2.4 that

$$\left|\frac{x^\gamma}{x}\right| < 1 \text{ for all } \gamma \in \mathrm{Gal}(K_{(N)}/K) \setminus \{\mathrm{id}\}. \tag{4.2}$$

To this end we consider by Proposition 3.1 and Proposition 3.2 a conjugate x^γ of x which is of the form

$$x^\gamma = \big(g_{(0,\frac{1}{N})}^{\frac{-12N}{\gcd(6,N)}}\big)^{\alpha\cdot\beta_Q}(\theta_Q) = g_{(\frac{s}{N},\frac{t}{N})\beta_Q}^{\frac{-12N}{\gcd(6,N)}}(\theta_Q)$$

for some $\alpha = \pm\left(\begin{smallmatrix} t-Bs & -Cs \\ s & t\end{smallmatrix}\right) \in W_{N,\theta}/\{\pm 1_2\}$, where $\mathrm{irr}(\theta, K) = X^2+BX+C$ and $Q = aX^2+bXY+cY^2$ is a reduced quadratic form of discriminant d_K. If $a \geq 2$, the inequality (4.2) holds by Lemma 4.2. If $a = 1$, we derive from the condition (3.2) and (3.3) that

$$Q = \begin{cases} X^2 - \frac{d_K}{4}Y^2 & \text{for} \quad d_K \equiv 0 \pmod 4 \\ X^2 + XY + \frac{1-d_K}{4}Y^2 & \text{for} \quad d_K \equiv 1 \pmod 4, \end{cases} \tag{4.3}$$

which yields $\beta_Q \equiv 1_2 \pmod N$ by the relations (3.6) and (3.7). Hence $x^\gamma = g_{(\frac{s}{N},\frac{t}{N})}^{\frac{-12N}{\gcd(6,N)}}(\theta_Q)$. Moreover, if $(s,t) \not\equiv (0,\pm 1) \pmod N$, then the inequality (4.2) is also true by Lemma 4.3 and Lemma 4.4. Here it is not necessary to consider the remaining case where $a = 1$ and $(s,t) \equiv (0, \pm 1) \pmod N$, because $\gamma = \mathrm{id} \in \mathrm{Gal}(K_{(N)}/K)$ in this case. Therefore (4.2) holds for all $\gamma \in \mathrm{Gal}(K_{(N)}/K) \setminus \{\mathrm{id}\}$ as desired. □

Remark 4.6. Note that the fields $\mathbb{Q}(\sqrt{-2})$, $\mathbb{Q}(\sqrt{-7})$, $\mathbb{Q}(\sqrt{-11})$ and $\mathbb{Q}(\sqrt{-19})$ have class number 1([1]). For such a field K there is only one reduced quadratic form of discriminant d_K as in (4.3). Hence Theorem 4.5 is true for this K and all $N \geq 2$, because we don't need to apply Lemma 4.2 in the proof. Lastly we list the other fields K and integers N which cannot be covered by our argument as follows:

Table 1. Exceptions of Theorem 4.5

K	d_K	(N, a singular value whose conjugates form a normal basis of $K_{(N)}$ over K)
$\mathbb{Q}(\sqrt{-15})$	-15	$(5,\ g_{(0,\frac{1}{5})}^{-60}(\frac{-1+\sqrt{-15}}{2}))$, $(6,\ g_{(0,\frac{1}{6})}^{-12}(\frac{-1+\sqrt{-15}}{2}))$, $(7,\ g_{(0,\frac{1}{7})}^{-84}(\frac{-1+\sqrt{-15}}{2}))$, $(8,\ g_{(0,\frac{1}{8})}^{-48}(\frac{-1+\sqrt{-15}}{2}))$
$\mathbb{Q}(\sqrt{-5})$	-20	$(5,\ g_{(0,\frac{1}{5})}^{-60}(\sqrt{-5}))$, $(6,\ g_{(0,\frac{1}{6})}^{-12}(\sqrt{-5}))$
$\mathbb{Q}(\sqrt{-23})$	-23	$(5,\ g_{(0,\frac{1}{5})}^{-60}(\frac{-1+\sqrt{-23}}{2}))$
$\mathbb{Q}(\sqrt{-6})$	-24	$(5,\ g_{(0,\frac{1}{5})}^{-60}(\sqrt{-6}))$

Even in these remaining 8 cases, however, one can verify Theorem 4.5 by numerical computation. For example, let $K = \mathbb{Q}(\sqrt{-5})$ and $N = 6$. Then $d_K = -20$, $\theta = \sqrt{-5}$ and

$$\begin{aligned}
&C(d_K) = \{Q_1 = X^2 + 5Y^2, \quad Q_2 = 2X^2 + 2XY + 3Y^2\}\\
&\theta_{Q_1} = \sqrt{-5}, \quad \theta_{Q_2} = \tfrac{-1+\sqrt{-5}}{2}\\
&\beta_{Q_1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \beta_{Q_2} = \begin{pmatrix} 1 & 5 \\ 3 & 2 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1_2\}\\
&W_{N,\theta}/\{\pm 1_2\} = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 2 & 3 \\ 3 & 2 \end{pmatrix}, \begin{pmatrix} 3 & 2 \\ 2 & 3 \end{pmatrix} \right\} \subset \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1_2\}.
\end{aligned}$$

If $x = g_{(0,\frac{1}{N})}^{\frac{-12N}{\gcd(6,N)}}(\theta) = g_{(0,\frac{1}{6})}^{-12}(\sqrt{-5})$, then by Proposition 3.1 and Proposition 3.2 its conjugates are

$$\begin{array}{llll}
x_1 = x, & x_2 = g_{(\frac{1}{6},0)}^{-12}(\sqrt{-5}), & x_3 = g_{(\frac{3}{6},\frac{2}{6})}^{-12}(\sqrt{-5}), & x_4 = g_{(\frac{2}{6},\frac{3}{6})}^{-12}(\sqrt{-5}) \\
x_5 = g_{(\frac{3}{6},\frac{2}{6})}^{-12}(\frac{-1+\sqrt{-5}}{2}), & x_6 = g_{(\frac{1}{6},\frac{5}{6})}^{-12}(\frac{-1+\sqrt{-5}}{2}), & x_7 = g_{(\frac{3}{6},\frac{1}{6})}^{-12}(\frac{-1+\sqrt{-5}}{2}), & x_8 = g_{(\frac{5}{6},\frac{4}{6})}^{-12}(\frac{-1+\sqrt{-5}}{2})
\end{array}$$

possibly with certain multiplicity. Hence by using MAPLE one can check that

$$\left|\frac{x_i}{x_1}\right| < 10^{-4} < \frac{1}{\#\mathrm{Gal}(K_{(6)}/K)} = \frac{1}{8} \quad \text{for } i = 2, \cdots, 8.$$

Therefore $\{x_1, \cdots, x_8\}$ becomes a normal basis of $K_{(6)}$ over K by Theorem 2.4. Moreover, one can also show that the minimal polynomial of x would be

$$\begin{aligned}
(X - x_1)\cdots(X - x_8) \;=\; & X^8 - 1263840X^7 + 42016796X^6 + 72894400X^5 \\
& +15056640X^4 - 4525280X^3 + 167196X^2 - 1280X + 1
\end{aligned}$$

with integer coefficients([5]).

References

1. D. A. Cox, *Primes of the form $x^2 + ny^2$: Fermat, Class Field, and Complex Multiplication*, John Wiley & Sons, Inc., 1989.
2. A. Gee, *Class invariants by Shimura's reciprocity law*, J. Theor. Nombres Bordeaux 11 (1999), no. 1, 45-72.
3. H. Y. Jung, J. K. Koo and D. H. Shin, *On some ray class invariants over imaginary quadratic fields*, submitted.
4. K. Komatsu, *Construction of a normal basis by special values of Siegel modular functions*, Proc. Amer. Math. Soc. 128 (2000), no. 2, 315-323.
5. J. K. Koo and D. H. Shin, *On some arithmetic properties of Siegel functions*, submitted.
6. D. Kubert and S. Lang, *Modular Units*, Grundlehren der mathematischen Wissenschaften 244, Spinger-Verlag, 1981.
7. S. Lang, *Elliptic Functions, 2nd edition*, Spinger-Verlag, 1987.
8. H. W. Leopoldt, *Über die Hauptordnung der ganzen Elemente eines abelschen Zahlkörpers*, J. Reine Angew. Math. 201 (1959) 119-149.
9. T. Okada, *On an extension of a theorem of S. Chowla*, Acta Arith. 38 (1980/81), no. 4, 341-345.
10. T. Okada, *Normal bases of class field over Gauss' number field*, J. London Math. Soc. (2) 22 (1980), no. 2, 221-225.
11. R. Schertz, *Galoismodulstruktur und elliptische Funktionen*, J. Number Theory 39 (1991), no. 3, 285-326
12. G. Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions*, Iwanami Shoten and Princeton University Press, 1971.
13. M. J. Talyor, *Relative Galois module structure of rings of integers and elliptic functions II*, Ann. of Math. (2) 121 (1985), no. 3, 519-535.
14. B. L. van der Waerden, *Algebra, Vol I*, Springer, 2003.

Department of Mathematical Sciences, KAIST
Current address: Taejon 373-1, Korea
E-mail address: `DOSAL@math.kaist.ac.kr`

Department of Mathematical Sciences, KAIST
Current address: Taejon 373-1, Korea
E-mail address: `jkkoo@math.kaist.ac.kr`

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