On some arithmetic properties of Siegel functions (II)

Ho Yun Jung, Ja Kyung Koo and Dong Hwa Shin

Abstract

Let K be an imaginary quadratic field other than $\mathbb{Q}(\sqrt{-1})$ and $\mathbb{Q}(\sqrt{-3})$ with discriminant d_K. We first construct primitive generators of the ring class fields over K of the orders of certain bounded conductors depending on d_K by making use of the singular values of Siegel functions unlike the classical cases. Next, denoting by $K_{(N)}$ the ray class field modulo N of K for an integer $N \geqslant 2$ we consider the field extension $K_{(p^2m)}/K_{(pm)}$ for a prime $p \geqslant 5$ and an integer $m \geqslant 1$ relatively prime to p and then find normal bases of all intermediate fields over $K_{(pm)}$ also via the singular values of Siegel functions as algebraic integers. Furthermore, we investigate certain Galois module structure of the field extension $K_{(p^n m)}/K_{(p^\ell m)}$ with $n \geqslant 2\ell$, which would be an extension of Komatsu's work([Kom94]).

1. Introduction

Let K be an imaginary quadratic field and $H_\mathcal{O}$ be the ring class field of the order $\mathcal{O}$ of conductor $N \geqslant 2$ in K. In number theory the ring class fields over imaginary quadratic fields play an important role in the study of certain quadratic Diophantine equations. For example, let n be a positive integer and $H_\mathcal{O}$ be the ring class field of the order $\mathcal{O} = \mathbb{Z}[\sqrt{-n}]$ in $K = \mathbb{Q}(\sqrt{-n})$. If p is an odd prime not dividing n, then we have the following assertions:

$$\begin{aligned} & p = x^2 + ny^2 \text{ is solvable for some integers } x \text{ and } y \\ \iff & p \text{ splits completely in } H_\mathcal{O} \\ \iff & \begin{cases} \text{the Legendre symbol } \left(\frac{-n}{p}\right) = 1 \text{ and} \\ f_n(X) \equiv 0 \pmod{p} \text{ has an integer solution} \end{cases} \end{aligned}$$

where $f_n(X)$ is the minimal polynomial of a real algebraic integer α for which $H_\mathcal{O} = K(\alpha)$([Cox89]).

Given an imaginary quadratic field K, it is a classical result by the main theorem of complex multiplication that for any proper fractional $\mathcal{O}$-ideal $\mathfrak{a}$, the j-invariant $j(\mathfrak{a})$ is an algebraic integer and generates $H_\mathcal{O}$ over K([Lan87] or [Shi71]). Unlike the classical case, however, Chen-Yui([CY96]) constructed a generator of the ring class field of certain conductor in terms of the singular value of the Thompson series which is a Hauptmodul for $\Gamma_0(N)$ or $\Gamma_0(N)^\dagger$. Here, $\Gamma_0(N) = \left\{\gamma \in \mathrm{SL}_2(\mathbb{Z}) : \gamma \equiv \left(\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right) \pmod{N}\right\}$ and $\Gamma_0^\dagger(N)$ is the subgroup of $\mathrm{SL}_2(\mathbb{R})$ generated by $\Gamma_0(N)$ and $\begin{pmatrix} 0 & -1/\sqrt{N} \\ \sqrt{N} & 0 \end{pmatrix}$. Similarly, Cox-Mckay-Stevenhagen([CMS04]) showed that certain singular value of a Hauptmodul for $\Gamma_0(N)$ or $\Gamma_0(N)^\dagger$ with rational Fourier coefficients generates $H_\mathcal{O}$ over K. Furthermore, Cho-Koo([CK]) recently revisited and extended their results by using the theory of Shimura's canonical models and his reciprocity law. On the other hand, as we see in the above example, it is essential to find the minimal polynomial of $j(\mathcal{O})$ over K, namely, the *class equation* of $\mathcal{O}$ in order to solve such quadratic equations. Although there are several known algorithms for finding the class

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

Keywords: class fields, modular forms and functions, normal bases, normal p-integral bases, Siegel functions

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

equations([CY96], [Cox89], [KY91], [Mor88]), these seem to be more or less complicated to calculate or inconvenient in practical use.

In this paper we shall first construct a ring class invariant of $H_{\mathcal{O}}$ over K under the condition

$$d_K \leqslant -43 \quad \text{and} \quad 2 \leqslant N \leqslant \frac{-\sqrt{3}\pi}{\ln\left(1-2.16e^{-\frac{\pi\sqrt{-d_K}}{24}}\right)}$$

in terms of the singular values of Siegel functions and also systematically find its minimal polynomial(Theorem 4.5, Remark 4.7, Theorem 3.5 and Remark 4.8) by adopting Gee's idea([Gee99]).

Next, as for normal bases, after Okada([Oka80]) had constructed normal bases of the ray class fields over the Gaussian field $\mathbb{Q}(\sqrt{-1})$, several other people treated the problem of generating normal bases of abelian extensions of other imaginary quadratic fields by special values of elliptic functions or elliptic modular functions([Cha87], [Kom94], [Sch91], [Tay85]). And, Jung-Koo-Shin([JKS]) recently found normal bases of the ray class fields over any imaginary quadratic field with discriminant $\leqslant -7$ by utilizing Siegel functions. We shall consider in this paper the extension $K_{(p^2m)}/K_{(pm)}$ for a prime $p \geqslant 5$ and an integer $m \geqslant 1$ relatively prime to p and construct a normal basis of F over $K_{(pm)}$ for each intermediate field F via the singular values of Siegel functions as algebraic integers(Theorem 5.7 and Theorem 5.8). And, we shall further discuss in Section 6 certain Galois module structure of the ring of p-integers of $K_{(p^nm)}$ over that of $K_{(p^\ell m)}$ where n and ℓ are positive integers with $n \geqslant 2\ell$, which is motivated by a relation between the existence of normal basis in $\mathbb{Z}_p$-extension and Greenberg's conjecture([FN91], [FK91]).

2. Field of modular functions

In this section we briefly review some necessary arithmetic properties of Siegel functions as modular functions.

For a positive integer N, let $\zeta_N = e^{\frac{2\pi i}{N}}$ and $\mathcal{F}_N$ be the field of modular functions of level N whose Fourier coefficients with respect to $e^{\frac{2\pi i\tau}{N}}(\tau \in \mathfrak{H} = \{\tau \in \mathbb{C} : \mathrm{Im}(\tau) > 0\})$ belong to $\mathbb{Q}(\zeta_N)$. Then $\mathcal{F}_N$ is a Galois extension of $\mathcal{F}_1 = \mathbb{Q}(j(\tau))(j$=the elliptic modular function) whose Galois group is isomorphic to $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)\}$. In order to describe the Galois action on the field $\mathcal{F}_N$ we consider the decomposition of the group

$$\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)\} = \{\left(\begin{smallmatrix}1&0\\0&d\end{smallmatrix}\right) : d \in (\mathbb{Z}/N\mathbb{Z})^*\} \cdot \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)\}.$$

Here, the matrix $\left(\begin{smallmatrix}1&0\\0&d\end{smallmatrix}\right)$ acts on $\sum_{n=-\infty}^{\infty} c_n e^{\frac{2\pi in\tau}{N}} \in \mathcal{F}_N$ by

$$\sum_{n=-\infty}^{\infty} c_n e^{\frac{2\pi in\tau}{N}} \mapsto \sum_{n=-\infty}^{\infty} c_n^{\sigma_d} e^{\frac{2\pi in\tau}{N}} \tag{2.1}$$

where σ_d is the automorphism of $\mathbb{Q}(\zeta_N)$ induced by $\zeta_N \mapsto \zeta_N^d$. And, for an element $\gamma \in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)\}$ let $\gamma' \in \mathrm{SL}_2(\mathbb{Z})$ be a preimage of γ via the natural surjection $\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})\{\pm\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)\}$. Then γ acts on $h \in \mathcal{F}_N$ by composition

$$h \mapsto h \circ \gamma' \tag{2.2}$$

as linear fractional transformation([Lan87] or [Shi71]).

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 $\mathfrak{H}$ by the following Fourier expansion

$$g_{(r_1,r_2)}(\tau) = -q_\tau^{\frac{1}{2}\mathbf{B}_2(r_1)} e^{\pi i r_2(r_1-1)}(1-q_z)\prod_{n=1}^{\infty}(1-q_\tau^n q_z)(1-q_\tau^n q_z^{-1}) \tag{2.3}$$

where $\mathbf{B}_2(X) = X^2 - X + \frac{1}{6}$ is the second Bernoulli polynomial, $q_\tau = e^{2\pi i\tau}$ and $q_z = e^{2\pi iz}$ with

$z = r_1\tau + r_2$. Then it is a modular unit which has no zeros and poles on $\mathfrak{H}$([KL81]). For later use we introduce some arithmetic properties and a modularity condition of Siegel functions:

Proposition 2.1. *Let $r = (r_1, r_2) \in \mathbb{Q}^2 \setminus \mathbb{Z}^2$. Then*

(i) *$g_r(\tau)$ is integral over $\mathbb{Z}[j(\tau)]$.*

(ii) *Let N be the smallest positive integer with $Nr \in \mathbb{Z}^2$. If N has at least two prime factors, then $1/g_r(\tau)$ is integral over $\mathbb{Z}[j(\tau)]$. If $N = p^s$ is a prime power, then $1/g_r(\tau)$ is integral over $\mathbb{Z}[\frac{1}{p}][j(\tau)]$.*

(iii) *For $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ we get*

$$g_r^{12}(\tau) \circ \gamma = g_{r\gamma}^{12}(\tau).$$

(iv) *For $s = (s_1, s_2) \in \mathbb{Z}^2$ we have*

$$g_{r+s}(\tau) = (-1)^{s_1s_2+s_1+s_2} e^{-\pi i(s_1r_2-s_2r_1)} g_r(\tau).$$

Proof. See [KS] Section 3 and Proposition 2.4. □

Proposition 2.2. *Let $N \geqslant 2$. Let $\{m(r)\}_{r\in\frac{1}{N}\mathbb{Z}^2\setminus\mathbb{Z}^2}$ be a family of integers such that $m(r) = 0$ except finitely many r. Then a product of Siegel functions*

$$\prod_{r\in\frac{1}{N}\mathbb{Z}^2\setminus\mathbb{Z}^2} g_r^{m(r)}(\tau)$$

belongs to $\mathcal{F}_N$, if $\{m(r)\}$ satisfies

$$\begin{aligned}
&\textstyle\sum_r m(r)(Nr_1)^2 \equiv \sum_r m(r)(Nr_2)^2 \equiv 0 \pmod{\gcd(2,N)\cdot N}\\
&\textstyle\sum_r m(r)(Nr_1)(Nr_2) \equiv 0 \pmod{N}\\
&\textstyle\gcd(12,N)\cdot\sum_r m(r) \equiv 0 \pmod{12}.
\end{aligned}$$

Proof. See [KL81] Chapter 3 Theorem 5.2 and 5.3. □

Corollary 2.3. *Let $N \geqslant 2$. For $r = (r_1, r_2) \in \frac{1}{N}\mathbb{Z}^2 \setminus \mathbb{Z}^2$ the function $g_r^{\frac{12N}{\gcd(6,N)}}(\tau)$ satisfies*

$$g_{(r_1,r_2)}^{\frac{12N}{\gcd(6,N)}}(\tau) = g_{(-r_1,-r_2)}^{\frac{12N}{\gcd(6,N)}}(\tau) = g_{(\langle r_1\rangle,\langle r_2\rangle)}^{\frac{12N}{\gcd(6,N)}}(\tau)$$

where $\langle X\rangle$ is the fractional part of $X \in \mathbb{R}$ so that $0 \leqslant \langle X\rangle < 1$. It belongs to $\mathcal{F}_N$ and γ in $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)\} \cong \mathrm{Gal}(\mathcal{F}_N/\mathcal{F}_1)$ acts on the function by

$$\left(g_r^{\frac{12N}{\gcd(6,N)}}(\tau)\right)^\gamma = g_{r\gamma}^{\frac{12N}{\gcd(6,N)}}(\tau).$$

Proof. It is a direct consequence of Proposition 2.1, Proposition 2.2 and definition (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.

Let $K(\neq \mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-3}))$ be an imaginary quadratic field of discriminant d_K and define

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

which is a generator of the ring of integers $\mathcal{O}_K$ of K, that is, $\mathcal{O}_K = \mathbb{Z}[\theta]$. We denote by H the Hilbert class field. Utilizing the Shimura's reciprocity law Gee([Gee99]) described the actions of

$\mathrm{Gal}(K_{(N)}/H)$ and $\mathrm{Gal}(H/K)$ explicitly. By extending her idea we shall examine $\mathrm{Gal}(H_{\mathcal{O}}/K)$ for the order $\mathcal{O}$ of conductor N.

Under the properly equivalent relation primitive positive 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* primitive positive definite quadratic forms, which are characterized by the conditions

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

together with the discriminant relation

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

Then from the above two conditions for reduced quadratic forms one can deduce

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

And, for a reduced quadratic form $Q=aX^2+bXY+cY^2\in C(d_K)$ we define a CM-point by

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

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

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

and

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

It is then well-known that $C(d_K)$ is isomorphic to $\mathrm{Gal}(H/K)$ and the action of Q on H can be extended to that on $K_{(N)}$ as

$$\begin{aligned}\mathrm{Gal}(H/K)\cong C(d_K) &\hookrightarrow \mathrm{Gal}(K_{(N)}/K)\\ Q &\mapsto \big(h(\theta)\mapsto h^{\beta_Q}(\theta_Q)\big)\end{aligned} \tag{3.8}$$

where h is an element of $\mathcal{F}_N$, defined and finite at θ. Here we observe that

$$K_{(N)}=K\big(h(\theta)\ :\ h\in\mathcal{F}_N \text{ is defined and finite at } \theta\big) \tag{3.9}$$

by the main theorem of complex multiplication([Lan87] or [Shi71]) and there exists $\beta\in\mathrm{GL}_2^+(\mathbb{Q})\cap\mathrm{M}_2(\mathbb{Z})$ such that $\beta\equiv\beta_p \pmod{N\mathbb{Z}_p}$ for all primes p dividing N by the Chinese remainder theorem. Thus the action of β_Q on $\mathcal{F}_N$ is understood as that of β which is an element of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\big\{\pm\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)\big\}$([Shi71] or [Gee99]).

Let

$$\mathrm{irr}(\theta,\ K)=X^2+B_\theta X+C_\theta=\begin{cases}X^2-\frac{d_K}{4} & \text{for}\quad d_K\equiv 0\pmod 4\\ X^2+X+\frac{1-d_K}{4} & \text{for}\quad d_K\equiv 1\pmod 4.\end{cases}$$

By the Shimura's reciprocity law we have an isomorphism

$$\begin{aligned}W_{N,\theta}/\big\{\pm\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)\big\} &\xrightarrow{\sim} \mathrm{Gal}(K_{(N)}/H)\\ \gamma &\mapsto \big(h(\theta)\mapsto h^{\gamma}(\theta)\big)\end{aligned} \tag{3.10}$$

where $h \in \mathcal{F}_N$ is defined and finite at θ, and $W_{N,\theta} = \left\{ \left(\begin{smallmatrix} t-B_\theta s & -C_\theta s \\ s & t \end{smallmatrix} \right) \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) \right\} / \left\{ \pm \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix} \right) \right\}$([Shi71] or [Gee99]).

The following two lemmas were originally studied in [KS], but we give their proofs for completeness of arguments.

Lemma 3.1. *For $N \geqslant 2$, let A and D be positive integers such that $AD = N$ and $D \geqslant 2$. Then $N\theta$ and $\frac{A\theta+B}{D}$ are not equivalent under $\mathrm{SL}_2(\mathbb{Z})$ for any integer B.*

Proof. Suppose on the contrary that $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix} \right) (N\theta) = \frac{A\theta+B}{D}$ for some $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix} \right) \in \mathrm{SL}_2(\mathbb{Z})$. Then by using the identity in [Sil94] Lemma 1.1 we have

$$\mathrm{Im}\big(\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix} \right) (N\theta)\big) = \tfrac{N}{|cN\theta+d|^2}\mathrm{Im}(\theta) = \mathrm{Im}\big(\tfrac{A\theta+B}{D}\big) = \tfrac{A}{D}\mathrm{Im}(\theta),$$

which yields $ND = A|cN\theta + d|^2 = Ac^2N^2|\theta|^2 + 2AcdN\mathrm{Re}(\theta) + Ad^2$. Replacing N by AD and dividing the equation by A we derive

$$D^2 = A^2D^2c^2|\theta|^2 + 2ADcd\mathrm{Re}(\theta) + d^2. \tag{3.11}$$

On the other hand, we have $\mathrm{Re}(\theta) = 0,\ -\frac{1}{2}$ by the definition (3.1), and $|\theta|^2 \geqslant 2$ from the fact $K \neq \mathbb{Q}(\sqrt{-1}),\ \mathbb{Q}(\sqrt{-3})$.

If $\mathrm{Re}(\theta) = 0$, then (3.11) is reduced to $D^2 = A^2D^2c^2|\theta|^2 + d^2$. Thus D divides d so that putting $d = De$ and dividing both sides by D^2 we get $1 = A^2c^2|\theta|^2 + e^2$. Since $|\theta|^2 \geqslant 2$, we have $c = 0$ and $e = \pm 1$; hence $\gcd(c, d) = D \geqslant 2$. But this contradicts the fact $ad - bc = 1$.

If $\mathrm{Re}(\theta) = -\frac{1}{2}$, then (3.11) becomes $D^2 = A^2D^2c^2|\theta|^2 - ADcd + d^2$. And D divides d^2, which implies $d \neq \pm 1$ because $D \geqslant 2$. On the other hand, since $|\theta|^2 \geqslant 2$, we get $D^2 \geqslant 2A^2D^2c^2 - ADcd + d^2 = \big(\frac{7A^2c^2}{4}\big)D^2 + \big(\frac{ADc}{2} - d\big)^2$. This yields $c = 0$ so that $\gcd(c, d) = |d| > 1$. However, it again contradicts $ad - bc = 1$. Therefore $N\theta$ and $\frac{A\theta+B}{D}$ can not be equivalent under $\mathrm{SL}_2(\mathbb{Z})$. □

Lemma 3.2. *Let $N \geqslant 2$. If the function $j(N\tau)$ satisfies $j(N\theta) = j(N\tau) \circ \alpha(\theta)$ for some $\alpha = \left(\begin{smallmatrix} x & y \\ z & w \end{smallmatrix} \right) \in \mathrm{SL}_2(\mathbb{Z})$, then $z \equiv 0 \pmod N$, that is, $\alpha \in \Gamma_0(N)$.*

Proof. Note that $j(N\tau) \circ \alpha(\theta) = j \circ \left(\begin{smallmatrix} Nx & Ny \\ z & w \end{smallmatrix} \right) (\theta)$. Since $\left(\begin{smallmatrix} Nx & Ny \\ z & w \end{smallmatrix} \right)$ is a primitive matrix of determinant N, we can decompose it into $\beta \left(\begin{smallmatrix} A & B \\ 0 & D \end{smallmatrix} \right)$ for some $\beta \in \mathrm{SL}_2(\mathbb{Z})$ and positive integers A, B, D such that $AD = N$. Then $j(N\theta) = j \circ \left(\begin{smallmatrix} Nx & Ny \\ z & w \end{smallmatrix} \right) (\theta) = j \circ \beta \left(\begin{smallmatrix} A & B \\ 0 & D \end{smallmatrix} \right) (\theta) = j \circ \left(\begin{smallmatrix} A & B \\ 0 & D \end{smallmatrix} \right) (\theta) = j(\frac{A\theta+B}{D})$, which yields that $N\theta$ and $\frac{A\theta+B}{D}$ are equivalent under $\mathrm{SL}_2(\mathbb{Z})$. Now Lemma 3.1 forces us to have $D = 1$ and $A = N$, from which we achieve $z \equiv 0 \pmod N$ due to the fact $\left(\begin{smallmatrix} Nx & Ny \\ z & w \end{smallmatrix} \right) = \beta \left(\begin{smallmatrix} A & B \\ 0 & D \end{smallmatrix} \right)$. □

Theorem 3.3. *Let $\mathcal{O}$ be the order of conductor $N \geqslant 2$ in K. Then we obtain*

$$\mathrm{Gal}(H_{\mathcal{O}}/H) \cong W_{N,\theta} / \left\{ \left(\begin{smallmatrix} t & 0 \\ 0 & t \end{smallmatrix} \right) \ : \ t \in (\mathbb{Z}/N\mathbb{Z})^* \right\}.$$

Proof. As is well-known, $H_{\mathcal{O}} = K\big(j(N\theta)\big)$([Lan87] or [Shi71]). Let γ be an element of $W_{N,\theta}$ which is of the form $\left(\begin{smallmatrix} t & 0 \\ 0 & t \end{smallmatrix} \right)$ for some $t \in (\mathbb{Z}/N\mathbb{Z})^*$. If we decompose γ into $\left(\begin{smallmatrix} 1 & 0 \\ 0 & d \end{smallmatrix} \right) \beta$ for some $d \in (\mathbb{Z}/N\mathbb{Z})^*$ and $\beta \in \mathrm{SL}_2(\mathbb{Z})$, then we obviously achieve $\beta \in \Gamma_0(N)$. Since the function $j(N\tau)$ is a modular function for $\Gamma_0(N)$ with rational Fourier coefficients, we deduce by (3.10) that

$$j(N\theta)^\gamma = j(N\tau)^\gamma(\theta) = j(N\tau)^\beta(\theta) = j(N\tau) \circ \beta(\theta) = j(N\theta).$$

Conversely, assume that an element $\gamma = \left(\begin{smallmatrix} t-B_\theta s & -C_\theta s \\ s & t \end{smallmatrix} \right)$ in $W_{N,\theta}$ fixes $j(N\theta)$. Decompose γ into $\left(\begin{smallmatrix} 1 & 0 \\ 0 & d \end{smallmatrix} \right) \beta$ for some $d \in (\mathbb{Z}/N\mathbb{Z})^*$ and $\beta \in \mathrm{SL}_2(\mathbb{Z})$. By the same reasoning as above we derive $j(N\theta)^\gamma = j(N\tau) \circ \beta(\theta)$. On the other hand, we know $\beta \in \Gamma_0(N)$ by Lemma 3.2, and so $s \equiv 0 \pmod N$. Therefore $\gamma = \left(\begin{smallmatrix} t & 0 \\ 0 & t \end{smallmatrix} \right)$. This proves the theorem. □

Remark 3.4. We have the degree formula

$$[K_{(N)} : H] = \frac{\phi(N\mathcal{O}_K)w(N\mathcal{O}_K)}{w_K} \tag{3.12}$$

where ϕ is the Euler function for ideals, namely

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

for a power of prime ideal $\mathfrak{p}$, $w(N\mathcal{O}_K)$ is the number of roots of unity in K which are $\equiv 1 \pmod{N\mathcal{O}_K}$ and w_K is the number of roots of unity in K([KL81]). And, for the order $\mathcal{O}$ of conductor N we know the formula

$$[H_{\mathcal{O}} : H] = \frac{N}{[\mathcal{O}_K^* : \mathcal{O}^*]} \prod_{p \mid N} \left(1 - \left(\frac{d_K}{p}\right)\frac{1}{p}\right)$$

where $\left(\frac{d_K}{p}\right)$ is the Legendre symbol for an odd prime p and $\left(\frac{d_K}{2}\right)$ is the Kronecker symbol([Cox89]). Thus the second part of the proof depending on Lemma 3.2 can be also established by showing that

$$[K_{(N)} : H_{\mathcal{O}}] = \frac{[K_{(N)} : H]}{[H_{\mathcal{O}} : H]} = \left|\left\{ \left(\begin{smallmatrix} t & 0 \\ 0 & t \end{smallmatrix}\right) \ : \ t \in (\mathbb{Z}/N\mathbb{Z})^* \right\} / \left\{ \pm \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) \right\}\right|.$$

Theorem 3.5. *Let $\mathcal{O}$ be the order of conductor $N \geqslant 2$ in K and f be an element of $\mathcal{F}_N$ such that $f(\theta) \in H_{\mathcal{O}}$. Then*

$$\left\{ f^{\gamma \cdot \beta_Q}(\theta_Q) \ : \ \gamma \in W_{N,\theta} / \left\{ \left(\begin{smallmatrix} t & 0 \\ 0 & t \end{smallmatrix}\right) : t \in (\mathbb{Z}/N\mathbb{Z})^* \right\} \text{ and } Q \in C(d_K) \right\}$$

is the set of all conjugates of $f(\theta)$ under the action of $\mathrm{Gal}(H_{\mathcal{O}}/K)$.

Proof. The assertion follows from the following diagram:

$$\begin{array}{cl}
\underline{\text{Fields}} & \qquad \underline{\text{Galois groups}} \\
H_{\mathcal{O}} & \\
\Big| \Big) & \mathrm{Gal}(H_{\mathcal{O}}/H) \cong W_{N,\theta} / \left\{ \left(\begin{smallmatrix} t & 0 \\ 0 & t \end{smallmatrix}\right) \ : \ t \in (\mathbb{Z}/N\mathbb{Z})^* \right\} \quad \text{by Theorem 3.3} \\
H & \\
\Big| \Big) & \mathrm{Gal}(H/K) = \left\{ \left(h(\theta) \mapsto h^{\beta_Q}(\theta_Q)\right)\big|_H \ : \ Q \in C(d_K) \right\} \quad \text{by (3.8)} \\
K &
\end{array}$$

where h is an element of $\mathcal{F}_N$, defined and finite at θ. □

Remark 3.6. Theorem 3.5 and the transformation formulas in Corollary 2.3 enable us to find all conjugates of the singular value $\prod_{\substack{1 \leqslant w \leqslant \frac{N}{2} \\ \gcd(w,N)=1}} g_{(0,\frac{w}{N})}^{\frac{12N}{\gcd(6,N)}}(\theta)$, which will be used to prove our first main theorem.

4. Primitive generators of the ring class fields

Let $K \neq \mathbb{Q}(\sqrt{-1}),\ \mathbb{Q}(\sqrt{-3})$ be an imaginary quadratic field with $d_K \leqslant -7$ and let θ be defined as in (3.1) and $N \geqslant 2$. 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) $\left|\frac{1-\zeta_N}{1-A^{\frac{1}{DN}}}\right| > 1$.

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

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

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

Proof. See [JKS2] Lemma 4.1. □

Lemma 4.2. *Assume the condition*

$$d_K \leqslant -43 \quad \text{and} \quad 2 \leqslant N \leqslant \frac{-\sqrt{3}\pi}{\ln\left(1 - 2.16e^{-\frac{\pi\sqrt{-d_K}}{24}}\right)}. \tag{4.1}$$

Let $Q = aX^2 + bXY + cY^2$ *be a reduced primitive positive definite quadratic form of discriminant* d_K *and* θ_Q *be as in (3.5). If* $a \geqslant 2$, *then the inequality*

$$\left|\frac{g_{(0,\frac{w}{N})}(\theta)}{g_{(\frac{s}{N},\frac{t}{N})}(\theta_Q)}\right| < 1$$

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

Proof. We may assume $0 \leqslant s \leqslant \frac{N}{2}$ by Corollary 2.3. And, we have $2 \leqslant a \leqslant D$ by (3.4) because Q is a reduced primitive positive definite quadratic form. From the definition (2.3) we obtain that

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

Now we see from the fact $a \leqslant D$ and Lemma 4.1(i) that $|1-\zeta_N^w| < 2$ and

$$\begin{aligned}\left|1-e^{2\pi i(\frac{s}{N}\cdot\frac{-b+\sqrt{d_K}}{2a}+\frac{t}{N})}\right| &\geqslant \begin{cases} |1-\zeta_N^t| & \geqslant |1-\zeta_N| \quad \text{if } s=0 \\ |1-A^{\frac{s}{Na}}| & \geqslant |1-A^{\frac{1}{ND}}| \quad \text{if } s\neq 0\end{cases} \\ &\geqslant 1-A^{\frac{1}{ND}}.\end{aligned}$$

Therefore we achieve that

$$\begin{aligned}
\left|\frac{g_{(0,\frac{w}{N})}(\theta)}{g_{(\frac{s}{N},\frac{t}{N})}(\theta_Q)}\right| &< \frac{2A^{\frac{1}{2}(\mathbf{B}_2(0)-\frac{1}{2}\mathbf{B}_2(0))}}{1-A^{\frac{1}{ND}}}\prod_{n=1}^{\infty}\frac{(1+A^n)^2}{(1-A^{\frac{n}{D}})(1-A^{\frac{1}{D}(n-\frac{1}{2})})} \quad \text{by the facts } 2\leqslant a\leqslant D,\ 0\leqslant s\leqslant \tfrac{N}{2} \\
&< \frac{2A^{\frac{1}{24}}}{1-A^{\frac{1}{ND}}}\prod_{n=1}^{\infty}(1+A^n)^2(1+A^{\frac{n}{1.03D}})(1+A^{\frac{1}{1.03D}(n-\frac{1}{2})}) \quad \text{by Lemma 4.1(ii)} \\
&< \frac{2A^{\frac{1}{24}}}{1-A^{\frac{1}{ND}}}\prod_{n=1}^{\infty}e^{2A^n+A^{\frac{n}{1.03D}}+A^{\frac{1}{1.03D}(n-\frac{1}{2})}} \quad \text{by Lemma 4.1(iv)} \\
&= \frac{2A^{\frac{1}{24}}}{1-A^{\frac{1}{ND}}}e^{\frac{2A}{1-A}+\frac{A^{\frac{1}{1.03D}}+A^{\frac{1}{2.06D}}}{1-A^{\frac{1}{1.03D}}}} \leqslant \frac{2e^{-\frac{\pi\sqrt{-d_K}}{24}}}{1-e^{-\frac{\sqrt{3}\pi}{N}}}\,e^{\frac{2e^{-\sqrt{43}\pi}}{1-e^{-\sqrt{43}\pi}}+\frac{e^{-\frac{\sqrt{3}\pi}{1.03}}+e^{-\frac{\sqrt{3}\pi}{2.06}}}{1-e^{-\frac{\sqrt{3}\pi}{1.03}}}} \quad \text{by the fact } d_K\leqslant -43 \\
&< \frac{2.16e^{-\frac{\pi\sqrt{-d_K}}{24}}}{1-e^{-\frac{\sqrt{3}\pi}{N}}} < 1 \quad \text{by the condition (4.1).}
\end{aligned}$$

This proves the lemma. □

Lemma 4.3. *Assume the condition*

$$d_K \leqslant -43 \quad \text{and} \quad 2 \leqslant N \leqslant \sqrt{-d_K}. \tag{4.2}$$

Let $Q = X^2 + bXY + cY^2$ *be a reduced primitive positive definite quadratic form of discriminant*

d_K. Then we get the inequality

$$\left|\frac{g_{(0,\frac{w}{N})}(\theta)}{g_{(\frac{s}{N},\frac{t}{N})}(\theta_Q)}\right| < 1$$

for $w \in \mathbb{Z} \setminus N\mathbb{Z}$ and $(s,t) \in \mathbb{Z}^2 \setminus N\mathbb{Z}^2$ with $s \not\equiv 0 \pmod{N}$.

Proof. We may assume $1 \leqslant s \leqslant \frac{N}{2}$ by Corollary 2.3. Then we establish that

$$\begin{aligned}
\left|\frac{g_{(0,\frac{w}{N})}(\theta)}{g_{(\frac{s}{N},\frac{t}{N})}(\theta_Q)}\right| &< A^{\frac{1}{2}(\mathbf{B}_2(0)-\mathbf{B}_2(\frac{s}{N}))}\left|\frac{1-\zeta_N^w}{1-A^{\frac{s}{N}}}\right|\prod_{n=1}^{\infty}\frac{(1+A^n)^2}{(1-A^{n+\frac{s}{N}})(1-A^{n-\frac{s}{N}})} \quad \text{by (2.3)}\\
&< A^{\frac{1}{2}(\mathbf{B}_2(0)-\mathbf{B}_2(\frac{1}{N}))}\frac{2}{1-A^{\frac{1}{N}}}\prod_{n=1}^{\infty}\frac{(1+A^n)^2}{(1-A^n)(1-A^{n-\frac{1}{2}})} \quad \text{by } 1 \leqslant s \leqslant \tfrac{N}{2}\\
&< \frac{2A^{\frac{1}{2}(\frac{1}{N}-\frac{1}{N^2})}}{1-A^{\frac{1}{N}}}\prod_{n=1}^{\infty}(1+A^n)^2(1+A^{\frac{n}{1.03}})(1+A^{\frac{1}{1.03}(n-\frac{1}{2})}) \quad \text{by Lemma 4.1(iii)}\\
&< \frac{2A^{\frac{1}{4N}}}{1-A^{\frac{1}{N}}}\prod_{n=1}^{\infty}e^{2A^n+A^{\frac{n}{1.03}}+A^{\frac{1}{1.03}(n-\frac{1}{2})}} \quad \text{by the fact } N \geqslant 2 \text{ and Lemma 4.1(iv)}\\
&= \frac{2A^{\frac{1}{4N}}}{1-A^{\frac{1}{N}}}e^{\frac{2A}{1-A}+\frac{A^{\frac{1}{1.03}}+A^{\frac{1}{2.06}}}{1-A^{\frac{1}{1.03}}}} \leqslant \frac{2e^{-\frac{\pi\sqrt{-d_K}}{4N}}}{1-e^{\frac{-\pi\sqrt{-d_K}}{N}}}e^{\frac{2e^{-\sqrt{43}\pi}}{1-e^{-\sqrt{43}\pi}}+\frac{e^{-\frac{\sqrt{43}\pi}{1.03}}+e^{-\frac{\sqrt{43}\pi}{2.06}}}{1-e^{-\frac{\sqrt{43}\pi}{1.03}}}} \quad \text{by the fact } d_K \leqslant -43\\
&< \frac{2.0001e^{-\frac{\pi\sqrt{-d_K}}{4N}}}{1-e^{\frac{-\pi\sqrt{-d_K}}{N}}} \leqslant \frac{2.0001e^{-\frac{\pi}{4}}}{1-e^{-\pi}} < 1 \quad \text{by the fact } N \leqslant \sqrt{-d_K},
\end{aligned}$$

which proves the lemma. □

Remark 4.4. Observe that the condition (4.1) is stronger than (4.2), namely

$$\frac{-\sqrt{3}\pi}{\ln\left(1-2.16e^{-\frac{\pi\sqrt{-d_K}}{24}}\right)} < \sqrt{-d_K}.$$

Now we are ready to prove our main theorem about primitive generators of the ring class fields over K.

Theorem 4.5. *Assume the condition (4.1) and let $\mathcal{O}$ be the order of conductor N in K. Then the singular value*

$$\prod_{\substack{1\leqslant w\leqslant \frac{N}{2}\\ \gcd(w,N)=1}} g_{(0,\frac{w}{N})}^{\frac{12N}{\gcd(6,N)}}(\theta) \tag{4.3}$$

generates $H_{\mathcal{O}}$ over K. It is a real algebraic integer and its minimal polynomial has integer coefficients. In particular, if the conductor N has at least two prime factors, then it is a unit.

Proof. Let $g(\tau) = \prod_{\substack{1\leqslant w\leqslant \frac{N}{2}\\ \gcd(w,N)=1}} g_{(0,\frac{w}{N})}^{\frac{12N}{\gcd(6,N)}}(\tau)$. By (3.10) and Theorem 3.3 we have $\mathrm{Gal}(K_{(N)}/H_{\mathcal{O}}) \cong \left\{\left(\begin{smallmatrix} t & 0\\ 0 & t\end{smallmatrix}\right) : t \in (\mathbb{Z}/N\mathbb{Z})^*\right\}/\left\{\pm\left(\begin{smallmatrix} 1 & 0\\ 0 & 1\end{smallmatrix}\right)\right\}$, and hence

$$g(\theta) = \prod_{w} g_{(0,\frac{1}{N})}^{\frac{12N}{\gcd(6,N)}}(\tau)^{\left(\begin{smallmatrix} w & 0\\ 0 & w\end{smallmatrix}\right)}(\theta) = \prod_{w} g_{(0,\frac{1}{N})}^{\frac{12N}{\gcd(6,N)}}(\theta)^{\left(\begin{smallmatrix} w & 0\\ 0 & w\end{smallmatrix}\right)} = \mathbf{N}_{K_{(N)}/H_{\mathcal{O}}}\left(g_{(0,\frac{1}{N})}^{\frac{12N}{\gcd 6,N}}(\theta)\right)$$

by Corollary 2.3 and (3.10). Thus $g(\theta)$ belongs to $H_{\mathcal{O}}$. Now, if we show that the element of $\mathrm{Gal}(H_{\mathcal{O}}/K)$ fixing the value $g(\theta)$ is only the identity, then we can conclude by Galois theory that it generates $H_{\mathcal{O}}$ over K.

It follows from Theorem 3.5 that any conjugate of $g(\theta)$ is of the form

$$g^{\gamma\cdot\beta_Q}(\theta_Q)$$

for some $\gamma = \left(\begin{smallmatrix} t-B_\theta s & -C_\theta s \\ s & t \end{smallmatrix}\right) \in W_{N,\theta}$ and $Q = aX^2+bXY+cY^2 \in C(d_K)$. Assuming $g(\theta) = g^{\gamma\cdot\beta_Q}(\theta_Q)$ we derive

$$\prod_w g_{(0,\frac{w}{N})}^{\frac{12N}{\gcd(6,N)}}(\theta) = \prod_w g_{(0,\frac{w}{N})\gamma\beta_Q}^{\frac{12N}{\gcd(6,N)}}(\theta_Q)$$

by Corollary 2.3. Since $|g(\theta)| = |g^{\gamma\cdot\beta_Q}(\theta_Q)|$, Lemma 4.2 leads us to have $a = 1$. This yields

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

from the condition (3.2) and the relation (3.3); hence $\beta_Q = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ as an element of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ by definitions (3.6) and (3.7) and $\theta_Q = \theta$ by definition (3.5). And we see from Corollary 2.3 that

$$g(\theta) = g^{\gamma\cdot\beta_Q}(\theta_Q) = \prod_w g_{(0,\frac{w}{N})\gamma\beta_Q}^{\frac{12N}{\gcd(6,N)}}(\theta_Q) = \prod_w g_{(\frac{ws}{N},\frac{wt}{N})}^{\frac{12N}{\gcd(6,N)}}(\theta)$$

from which we get $s \equiv 0 \pmod N$ by Lemma 4.3. Therefore the pair of $\gamma = \left(\begin{smallmatrix} t & 0 \\ 0 & t \end{smallmatrix}\right)$ and $Q = \mathrm{id}$ represents the identity on $H_\mathcal{O}$(see the tower in the proof of Theorem 3.5), and hence $g(\theta)$ actually generates $H_\mathcal{O}$ over K.

On the other hand, we derive from the definition (2.3)

$$\begin{aligned} g(\theta) &= \prod_w \left\{ q_\theta^{\frac{1}{12}}(1-\zeta_N^w) \prod_{n=1}^{\infty}(1-q_\theta^n\zeta_N^w)(1-q_\theta^n\zeta_N^{-w}) \right\}^{\frac{12N}{\gcd(6,N)}} \\ &= \prod_w \left\{ q_\theta^{\frac{N}{\gcd(6,N)}} \left(2\sin\tfrac{w\pi}{N}\right)^{\frac{12N}{\gcd(6,N)}} \prod_{n=1}^{\infty}\left(1-2\cos\tfrac{2w\pi}{N}q_\theta^n + q_\theta^{2n}\right)^{\frac{12N}{\gcd(6,N)}} \right\}, \end{aligned}$$

and this claims that $g(\theta)$ is a real number. Furthermore, we see from Proposition 2.1(i) that the function $g(\tau)$ is integral over $\mathbb{Z}[j(\tau)]$. Since $j(\theta)$ is a real algebraic integer([Lan87] or [Shi71]), so is the value $g(\theta)$. And its minimal polynomial over K has integer coefficients. In particular, if N has at least two prime factors, the function $1/g(\tau)$ is also integral over $\mathbb{Z}[j(\tau)]$ by Proposition 2.1(ii); hence $g(\theta)$ becomes a unit. □

Remark 4.6. Since the proof of Theorem 4.5 depends only on Lemma 4.2 and 4.3 which do not include any power of singular values, any nonzero power of the value in (4.3) can be also a generator of $H_\mathcal{O}$ over K.

Remark 4.7. If N is an odd prime p, by the definition (2.3) and the identity

$$\frac{1-X^p}{1-X} = (1-\zeta_pX)(1-\zeta_p^2X)\cdots(1-\zeta_p^{p-1}X)$$

we have

$$\left(\prod_{\substack{1\leqslant w\leqslant \frac{p}{2} \\ \gcd(w,p)=1}} g_{(0,\frac{w}{p})}^{\frac{12p}{\gcd(6,p)}}(\theta)\right)^{2\gcd(6,p)} = \prod_{1\leqslant w\leqslant p-1} g_{(0,\frac{w}{p})}^{24p}(\theta) = \left(p^{24}\frac{\Delta(p\theta)}{\Delta(\theta)}\right)^p$$

where Δ is the discriminant function. Since it is well-known that the value $\frac{\Delta(p\theta)}{\Delta(\theta)}$ lies in the ring class field of the order of conductor p([Lan87] Chapter 12), it becomes a ring class invariant too under the condition (4.1).

Remark 4.8. Before we close this section, we would like to present an example which cannot be covered by our method due to violation of the condition (4.1).

Let $K=\mathbb{Q}(\sqrt{-5})$ and $N=12(=2^2\cdot 3)$. Then $d_K=-20$, $\theta=\sqrt{-5}$ and

$C(d_K)=\big\{Q_1=X^2+5Y^2,\quad Q_2=2X^2+2XY+3Y^2\big\}$

$\theta_{Q_1}=\sqrt{-5},\quad \theta_{Q_2}=\frac{-1+\sqrt{-5}}{2}$

$\beta_{Q_1}=\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right),\quad \beta_{Q_2}=\left(\begin{smallmatrix}1&5\\3&2\end{smallmatrix}\right)$

$W_{N,\theta}/\big\{\left(\begin{smallmatrix}t&0\\0&t\end{smallmatrix}\right)\ :\ t\in(\mathbb{Z}/N\mathbb{Z})^*\big\}=\big\{\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right),\ \left(\begin{smallmatrix}1&6\\6&1\end{smallmatrix}\right),\ \left(\begin{smallmatrix}2&9\\3&2\end{smallmatrix}\right),\ \left(\begin{smallmatrix}3&2\\2&3\end{smallmatrix}\right),\ \left(\begin{smallmatrix}3&4\\4&3\end{smallmatrix}\right),\ \left(\begin{smallmatrix}4&9\\3&4\end{smallmatrix}\right),\ \left(\begin{smallmatrix}6&7\\1&6\end{smallmatrix}\right),\ \left(\begin{smallmatrix}0&7\\1&0\end{smallmatrix}\right)\big\}.$

Now, the conjugates of

$$x=\prod_{\substack{1\leqslant w\leqslant \frac{N}{2}\\ \gcd(w,N)=1}} g_{(0,\frac{w}{N})}^{\frac{12N}{\gcd(6,N)}}(\theta)=g^{24}_{(0,\frac{1}{12})}(\sqrt{-5})g^{24}_{(0,\frac{5}{12})}(\sqrt{-5})$$

are as follows:

$$\begin{array}{ll}
x_1\ =g^{24}_{(0,\frac{1}{12})}(\sqrt{-5})g^{24}_{(0,\frac{5}{12})}(\sqrt{-5}), & x_2\ =g^{24}_{(\frac{6}{12},\frac{1}{12})}(\sqrt{-5})g^{24}_{(\frac{6}{12},\frac{5}{12})}(\sqrt{-5})\\
x_3\ =g^{24}_{(\frac{3}{12},\frac{2}{12})}(\sqrt{-5})g^{24}_{(\frac{3}{12},\frac{10}{12})}(\sqrt{-5}), & x_4\ =g^{24}_{(\frac{2}{12},\frac{3}{12})}(\sqrt{-5})g^{24}_{(\frac{10}{12},\frac{3}{12})}(\sqrt{-5})\\
x_5\ =g^{24}_{(\frac{4}{12},\frac{3}{12})}(\sqrt{-5})g^{24}_{(\frac{8}{12},\frac{3}{12})}(\sqrt{-5}), & x_6\ =g^{24}_{(\frac{3}{12},\frac{4}{12})}(\sqrt{-5})g^{24}_{(\frac{3}{12},\frac{8}{12})}(\sqrt{-5})\\
x_7\ =g^{24}_{(\frac{1}{12},\frac{6}{12})}(\sqrt{-5})g^{24}_{(\frac{5}{12},\frac{6}{12})}(\sqrt{-5}), & x_8\ =g^{24}_{(\frac{1}{12},0)}(\sqrt{-5})g^{24}_{(\frac{5}{12},0)}(\sqrt{-5})\\
x_9\ =g^{24}_{(\frac{3}{12},\frac{2}{12})}(\frac{-1+\sqrt{-5}}{2})g^{24}_{(\frac{3}{12},\frac{10}{12})}(\frac{-1+\sqrt{-5}}{2}), & x_{10}=g^{24}_{(\frac{9}{12},\frac{8}{12})}(\frac{-1+\sqrt{-5}}{2})g^{24}_{(\frac{9}{12},\frac{4}{12})}(\frac{-1+\sqrt{-5}}{2})\\
x_{11}=g^{24}_{(\frac{9}{12},\frac{7}{12})}(\frac{-1+\sqrt{-5}}{2})g^{24}_{(\frac{9}{12},\frac{11}{12})}(\frac{-1+\sqrt{-5}}{2}), & x_{12}=g^{24}_{(\frac{11}{12},\frac{4}{12})}(\frac{-1+\sqrt{-5}}{2})g^{24}_{(\frac{7}{12},\frac{8}{12})}(\frac{-1+\sqrt{-5}}{2})\\
x_{13}=g^{24}_{(\frac{1}{12},\frac{2}{12})}(\frac{-1+\sqrt{-5}}{2})g^{24}_{(\frac{5}{12},\frac{10}{12})}(\frac{-1+\sqrt{-5}}{2}), & x_{14}=g^{24}_{(\frac{3}{12},\frac{11}{12})}(\frac{-1+\sqrt{-5}}{2})g^{24}_{(\frac{3}{12},\frac{7}{12})}(\frac{-1+\sqrt{-5}}{2})\\
x_{15}=g^{24}_{(\frac{7}{12},\frac{5}{12})}(\frac{-1+\sqrt{-5}}{2})g^{24}_{(\frac{11}{12},\frac{1}{12})}(\frac{-1+\sqrt{-5}}{2}), & x_{16}=g^{24}_{(\frac{1}{12},\frac{5}{12})}(\frac{-1+\sqrt{-5}}{2})g^{24}_{(\frac{5}{12},\frac{1}{12})}(\frac{-1+\sqrt{-5}}{2})
\end{array}$$

possibly with multiplicity by Theorem 3.5 and Corollary 2.3. Hence the minimal polynomial of x over K would be

$$\begin{aligned}
&(X-x_1)\quad\cdots\quad(X-x_{16})\\
&=X^{16}-1597283771136X^{15}+2186853349741068862 00X^{14}-98979876039958285135 3280X^{13}\\
&+163579392201131175333969 5900X^{12}-14781704087536896778727383 83488X^{11}\\
&+813690304957218006590231416378248X^{10}-4647287791605145269746263262 47201600X^{9}\\
&+16711771593595129505769652415606317 8310X^{8}-915576399865022355779519648703147132 1600X^{7}\\
&-1741005988361268212050898857141924698 1752X^{6}-319841816817605518033309793652265500 23488X^{5}\\
&+5677583625730635496464554293769775900X^{4}-2249102100642965467076167124913280X^{3}\\
&+238110589893565910129238086200X^{2}-255097494247676082005 1136X+1.
\end{aligned}$$

And this polynomial is irreducible over K, so x is indeed a primitive generator of the ring class field of the order of conductor 12 in $\mathbb{Q}(\sqrt{-5})$. Moreover, x is a unit because the constant term is 1. Therefore, it would be worthwhile to check how much further one can release the condition (4.1).

5. Construction of normal bases

Given an imaginary quadratic field $K(\neq\mathbb{Q}(\sqrt{-1}),\ \mathbb{Q}(\sqrt{-3}))$ we consider the extension $K_{(p^2m)}/K_{(pm)}$ for a prime $p\geqslant 5$ and an integer $m\geqslant 1$ relatively prime to p. In this section we shall construct a normal basis of each intermediate field F over $K_{(pm)}$.

First we explicitly determine all intermediate fields F between $K_{(p^2m)}$ and $K_{(pm)}$. Let θ be as in (3.1) and set $\mathrm{irr}(\theta,\ K)=X^2+B_\theta X+C_\theta$. Then one can identify $\Gamma=\mathrm{Gal}(K_{(p^2m)}/K_{(pm)})$ with

$$\big\{\gamma=\left(\begin{smallmatrix}t-B_\theta s&-C_\theta s\\ s&t\end{smallmatrix}\right)\in\mathrm{GL}_2(\mathbb{Z}/p^2m\mathbb{Z})\ :\ \gamma\equiv\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)\pmod{pm}\big\}/\big\{\pm\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)\big\}$$

by (3.10). Since $[K_{(p^2m)}:K_{(pm)}]=p^2$ by the formula (3.12), we readily know by inspection that

$$\Gamma=\big\langle \begin{pmatrix} 1+pm & 0 \\ 0 & 1+pm \end{pmatrix} \big\rangle \times \big\langle \begin{pmatrix} 1-B_\theta pm & -C_\theta pm \\ pm & 1 \end{pmatrix} \big\rangle,$$

which shows that $\Gamma\cong(\mathbb{Z}/p\mathbb{Z})^2$. Hence an element of Γ is of the form

$$\begin{pmatrix} 1+pm & 0 \\ 0 & 1+pm \end{pmatrix}^k \begin{pmatrix} 1-B_\theta pm & -C_\theta pm \\ pm & 1 \end{pmatrix}^\ell = \begin{pmatrix} 1+(k-B_\theta\ell)pm & -C_\theta\ell pm \\ \ell pm & 1+kpm \end{pmatrix} \quad \text{for} \quad 0\leqslant k,\ \ell\leqslant p-1.$$

Set

$$\Gamma_{(k,\ell)}=\langle\gamma_{(k,\ell)}\rangle=\big\langle \begin{pmatrix} 1+(k-B_\theta\ell)pm & -C_\theta\ell pm \\ \ell pm & 1+kpm \end{pmatrix} \big\rangle \quad \text{for} \quad (k,\ell)\in\big\{(0,1),(1,0),(1,1),\cdots,(1,p-1)\big\},$$

which represents all subgroups of Γ of order p. And, let $F_{(k,\ell)}$ be its corresponding fixed field of $\Gamma_{(k,\ell)}$, namely

$$F_{(k,\ell)}=K_{(p^2m)}^{\Gamma_{(k,\ell)}} \quad \text{for} \quad (k,\ell)\in\big\{(0,1),(1,0),(1,1),\cdots,(1,p-1)\big\}.$$

Then we have the field tower:

$$\begin{tikzcd}
& & K_{(p^2m)} \arrow[dll, dash] \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] \arrow[drr, dash] & & \\
F_{(0,1)} \arrow[drr, dash] & F_{(1,0)} \arrow[dr, dash] & F_{(1,1)} \arrow[d, dash] & \cdots \arrow[dl, dash] & F_{(1,p-1)} \arrow[dll, dash] \\
& & K_{(pm)} & &
\end{tikzcd}$$

Lemma 5.1. *ζ_p, $g_{(0,\frac{1}{pm})}^{12pm}(\theta)\in K_{(pm)}$ and ζ_{p^2}, $g_{(0,\frac{1}{pm})}^{12m}(\theta)\in K_{(p^2m)}$.*

Proof. One can check by Proposition 2.2 that $g_{(0,\frac{1}{pm})}^{12pm}(\tau)\in\mathcal{F}_{pm}$ and $g_{(0,\frac{1}{pm})}^{12m}(\tau)\in\mathcal{F}_{p^2m}$. Hence we get the assertion by (3.9). □

Let us investigate the action of $\gamma_{(k,\ell)}$ on ζ_{p^2} and $g_{(0,\frac{1}{pm})}^{12m}(\theta)$. To this end we decompose $\gamma_{(k,\ell)}$ into

$$\begin{aligned}\gamma_{(k,\ell)}=\alpha_{(k,\ell)}\cdot\beta_{(k,\ell)}&=\begin{pmatrix} 1 & 0 \\ 0 & 1+(2k-B_\theta\ell)pm \end{pmatrix}\begin{pmatrix} 1+(k-B_\theta\ell)pm & -C_\theta\ell pm \\ \ell pm & 1+(B_\theta\ell-k)pm \end{pmatrix}\\ &\in\big\{\left(\begin{smallmatrix}1&0\\0&d\end{smallmatrix}\right)\ :\ d\in(\mathbb{Z}/p^2m\mathbb{Z})^*\big\}\cdot\mathrm{SL}_2(\mathbb{Z}/p^2m\mathbb{Z})/\big\{\pm\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)\big\}.\end{aligned}$$

We see directly from (2.3) that the function $g_{(0,\frac{1}{pm})}^{12m}(\tau)$ has Fourier coefficients in $\mathbb{Q}(\zeta_{pm})$. Thus the action of $\alpha_{(k,\ell)}$ is described by (3.10) and (2.1) as

$$\begin{aligned}\zeta_{p^2}&\mapsto\zeta_{p^2}^{1+(2k-B_\theta\ell)pm}\\ g_{(0,\frac{1}{pm})}^{12m}(\theta)&\mapsto g_{(0,\frac{1}{pm})}^{12m}(\theta).\end{aligned}$$

For some integers $A,\ B,\ C,\ D$ let

$$\beta'_{(k,\ell)}=\begin{pmatrix} 1+(k-B_\theta\ell)pm+p^2mA & -C_\theta\ell pm+p^2mB \\ \ell pm+p^2mC & 1+(B_\theta\ell-k)pm+p^2mD \end{pmatrix}$$

be a preimage of $\beta_{(k,\ell)}$ via the natural surjection $\mathrm{SL}_2(\mathbb{Z})\to\mathrm{SL}_2(\mathbb{Z}/p^2m\mathbb{Z})/\big\{\pm\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)\big\}$. Then by

(3.10) and (2.2) we derive that the action of $\beta_{(k,\ell)}$ is given by

$$\begin{aligned}\zeta_{p^2} &\mapsto \zeta_{p^2}\\ g^{12m}_{(0,\frac{1}{pm})}(\theta) &\mapsto g^{12m}_{(0,\frac{1}{pm})}(\tau)\circ\beta'_{(k,\ell)}(\theta) = g^{12m}_{(0,\frac{1}{pm})\beta'_{(k,\ell)}}(\theta) \quad \text{by Proposition 2.1(iii)}\\ &= g^{12m}_{(\ell+pC,\frac{1}{pm}+B_\theta\ell-k+pD)}(\theta) = \zeta_{p^2}^{-6p\ell} g^{12m}_{(0,\frac{1}{pm})}(\theta) \quad \text{by Proposition 2.1(iv).}\end{aligned}$$

Hence $\gamma_{(k,\ell)}$ maps

$$\zeta_{p^2} \mapsto \zeta_{p^2}^{1+(2k-B_\theta\ell)pm} \tag{5.1}$$

$$g^{12m}_{(0,\frac{1}{pm})}(\theta) \mapsto \zeta_{p^2}^{-6p\ell} g^{12m}_{(0,\frac{1}{pm})}(\theta). \tag{5.2}$$

Lemma 5.2. *Let $(k,\ell)\in\{(0,1),(1,0),(1,1),\cdots,(1,p-1)\}$. Then $\Gamma_{(k,\ell)}$ fixes $\zeta_{p^2}^x g^{12my}_{(0,\frac{1}{pm})}(\theta)$ for some $x,\ y\in\mathbb{Z}$ if and only if x and y satisfy*

$$\begin{cases} -B_\theta mx \equiv 6y \pmod p & \text{if } (k,\ell)=(0,1)\\ x \equiv 0 \pmod p & \text{if } (k,\ell)=(1,0)\\ (2-B_\theta\ell)mx \equiv 6\ell y \pmod p & \text{otherwise.}\end{cases} \tag{5.3}$$

Proof. It follows from (5.1) and (5.2) that

$$\big(\zeta_{p^2}^x g^{12my}_{(0,\frac{1}{pm})}(\theta)\big)^{\gamma_{(k,\ell)}} = \zeta_{p^2}^{(1+(2k-B_\theta\ell)pm)x-6p\ell y} g^{12my}_{(0,\frac{1}{pm})}(\theta).$$

Then this value is equal to $\zeta_{p^2}^x g^{12my}_{(0,\frac{1}{pm})}(\theta)$ if and only if

$$(1+(2k-B_\theta\ell)pm)x-6p\ell y \equiv x \pmod{p^2},$$

which reduces to (5.3). And, this proves the lemma. □

Lemma 5.3. $K_{(p^2m)} = K_{(pm)}\big(\zeta_{p^2},\ g^{12m}_{(0,\frac{1}{pm})}(\theta)\big)$.

Proof. Since $g^{12m}_{(0,\frac{1}{pm})}(\theta)\notin F_{(0,1)}$ and $g^{12m}_{(0,\frac{1}{pm})}(\theta)\in F_{(1,0)}$ by (5.2), we claim that $g^{12m}_{(0,\frac{1}{pm})}(\theta)\notin K_{(pm)}$ and $F_{(1,0)} = K_{(pm)}\big(g^{12m}_{(0,\frac{1}{pm})}(\theta)\big)$ owing to the fact $[F_{(1,0)}:K_{(pm)}]=p$. Furthermore, since $\zeta_{p^2}\notin F_{(1,0)}$ by (5.1), we achieve by the fact $[K_{(p^2m)}:F_{(1,0)}]=p$ that

$$K_{(p^2m)} = F_{(1,0)}\big(\zeta_{p^2}\big) = K_{(pm)}\big(\zeta_{p^2},\ g^{12m}_{(0,\frac{1}{pm})}(\theta)\big).$$

□

Theorem 5.4. *Let $(k,\ell)\in\{(0,1),(1,0),(1,1),\cdots,(1,p-1)\}$ and y' be the integer such that $y\cdot y'\equiv 1 \pmod p$ and $0<y'<p$ for an integer $y\not\equiv 0 \pmod p$. Then we have*

$$F_{(k,\ell)} = \begin{cases} K_{(pm)}\big(\zeta_{p^2} g^{12m^2 6'(p-B_\theta)}_{(0,\frac{1}{pm})}(\theta)\big) & \text{if } (k,\ell)=(0,1)\\ K_{(pm)}\big(g^{12m}_{(0,\frac{1}{pm})}(\theta)\big) & \text{if } (k,\ell)=(1,0)\\ K_{(pm)}\big(\zeta_{p^2} g^{12m^2(6\ell)'(2+p-B_\theta\ell)}_{(0,\frac{1}{pm})}(\theta)\big) & \text{otherwise.}\end{cases}$$

Proof. Take a solution of (5.3) as

$$(x,y) = \begin{cases} (1, m6'(p-B_\theta)) & \text{if } (k,\ell)=(0,1)\\ (0,1) & \text{if } (k,\ell)=(1,0)\\ (1, m(6\ell)'(2+p-B_\theta\ell)) & \text{otherwise}\end{cases} \tag{5.4}$$

which consists of nonnegative integers. We can then readily check that a solution (x,y) in (5.4) does not satisfy two congruence equations in (5.3) simultaneously. This shows that for each (x,y),

$\zeta_{p^2}^x g_{(0,\frac{1}{pm})}^{12my}(\theta)$ belongs to a unique $F_{(k,\ell)}$; hence in particular, it is not in $K_{(pm)}$. Since $[F_{(k,\ell)} : K_{(pm)}] = p$, we get the conclusion. □

To accomplish our goal we are in need of the following two lemmas:

Lemma 5.5. *Let L be a number field containing ζ_n and F be a cyclic extension over L of degree n. Then there exists an element ξ of L such that $F = L(\sqrt[n]{\xi})$. And, the conjugates of $\sum_{s=0}^{n-1}(\sqrt[n]{\xi})^s$ over L form a normal basis of F over L.*

Proof. See [Kaw84] p. 223. □

Lemma 5.6. *Let L be a number field. Let F_1 and F_2 be finite Galois extensions of L with $F_1 \cap F_2 = L$. If the conjugates of $\xi_s \in F_s$ over L form a normal basis of F_s over L for $s = 1,\ 2$, then the conjugates of $\xi_1\xi_2$ over L form a normal basis of F_1F_2 over L.*

Proof. See [Kaw84] p. 227. □

Now we are ready to prove our main theorem about normal bases.

Theorem 5.7. *Let (k,ℓ) and y' be as in Theorem 5.4. Then the conjugates of*

$$\begin{cases} \sum_{s=0}^{p-1}\left(\zeta_{p^2} g_{(0,\frac{1}{pm})}^{12m^2 6'(p-B_\theta)}(\theta)\right)^s & \textit{if} \quad (k,\ell) = (0,1) \\ \sum_{s=0}^{p-1} g_{(0,\frac{1}{pm})}^{12ms}(\theta) & \textit{if} \quad (k,\ell) = (1,0) \\ \sum_{s=0}^{p-1}\left(\zeta_{p^2} g_{(0,\frac{1}{pm})}^{12m^2(6\ell)'(2+p-B_\theta\ell)}(\theta)\right)^s & \textit{otherwise} \end{cases} \tag{5.5}$$

over $K_{(pm)}$ form a normal basis of $F_{(k,\ell)}$ over $K_{(pm)}$. Moreover, the values in (5.5) are algebraic integers.

Proof. Since the function $g_{(0,\frac{1}{pm})}(\tau)$ is integral over $\mathbb{Z}[j(\tau)]$ by Proposition 2.1(i) and $j(\theta)$ is an algebraic integer([Lan87] or [Shi71]), the values in (5.5) are all algebraic integers. Thus the theorem follows by applying Lemma 5.5 with the aid of Lemma 5.1 and Theorem 5.4. □

Theorem 5.8. *The conjugates of the algebraic integer*

$$\left(\sum_{s=0}^{p-1}\zeta_{p^2}^s\right)\left(\sum_{s=0}^{p-1} g_{(0,\frac{1}{pm})}^{12ms}(\theta)\right)$$

over $K_{(pm)}$ form a normal basis of $K_{(p^2m)}$ over $K_{(pm)}$.

Proof. If $F_1 = K_{(pm)}(\zeta_{p^2})$ and $F_2 = K_{(pm)}(g_{(0,\frac{1}{pm})}^{12m}(\theta))$, then $[F_s : K_{(pm)}] \leqslant p$ for $s = 1,\ 2$ by Lemma 5.1. On the other hand, Lemma 5.3 shows $F_1F_2 = K_{(p^2m)}$, from which we get $F_1 \cap F_2 = K_{(pm)}$ and $[F_s : K_{(pm)}] = p$ for $s = 1,\ 2$. Hence the conjugates of $\sum_{s=0}^{p-1}\zeta_{p^2}^s$ and $\sum_{s=0}^{p-1} g_{(0,\frac{1}{pm})}^{12ms}(\theta)$ over $K_{(pm)}$ form normal bases of F_1 and F_2, respectively, by Lemma 5.5 and Lemma 5.1. And, the theorem follows from Lemma 5.6. □

6. Galois module structure

Let L be a number field and p be an odd prime. We say that an extension L_∞/L is a $\mathbb{Z}_p$*-extension* of L if there exists a sequence of cyclic extensions of L

$$L = L_0 \subset L_1 \subset \cdots \subset L_n \subset \cdots \subset L_\infty = \cup_{n=0}^{\infty} L_n$$

with $\mathrm{Gal}(L_n/L)\cong\mathbb{Z}/p^n\mathbb{Z}$. Then it is well-known that L_∞/L is unramified outside p([Was96] Proposition 13.2). And, Greenberg([Gre76]) has conjectured that if L is totally real, then the Iwasawa λ-invariant of L_∞/L vanishes.

Denoting the ring of p-integers of L by $\mathcal{O}_L[\frac{1}{p}]$ we say that a finite Galois extension F of L has a *normal p-integral basis over L* if $\mathcal{O}_F[\frac{1}{p}]$ is a free $\mathcal{O}_L[\frac{1}{p}]\mathrm{Gal}(F/L)$-module of rank one. We then say that a $\mathbb{Z}_p$-extension L_∞ of L has a *normal basis over L* if each L_n has a normal p-integral basis over L.

On the other hand, we see from [Kom94] that there is a negative data for Greenberg's conjecture. For instance, for a positive square free integer d with $(\frac{-d}{3})=-1$, let $L=\mathbb{Q}(\sqrt{3d})$ and $L'=\mathbb{Q}(\sqrt{-d})$. It was shown in [FN91] and [FK91] that if 3 divides the class number of L and if every $\mathbb{Z}_3$-extension of L' has a normal basis, then the λ-invariant of the cyclotomic $\mathbb{Z}_3$-extension of L does not vanish. This suggests a relation between the existence of normal basis in $\mathbb{Z}_p$-extension and Greenberg's conjecture, which motivates this section.

Now, let $K(\neq\mathbb{Q}(\sqrt{-1}),\ \mathbb{Q}(\sqrt{-3}))$ be an imaginary quadratic field, $p\geqslant 5$ be a prime and $m\geqslant 1$ be an integer relatively prime to p. And, let n and ℓ be positive integers with $n\geqslant 2\ell$. Observe that the extension $K_{(p^nm)}/K_{(p^\ell m)}$ is unramified outside p and $\zeta_{p^n}\in K_{(p^nm)}$, $\zeta_{p^\ell}\in K_{(p^\ell m)}$ but $\zeta_{p^{n+1}}\notin K_{(p^nm)}$, $\zeta_{p^{\ell+1}}\notin K_{(p^\ell m)}$([KL81] Chapter 9 Lemma 4.3). We shall prove in this section that $K_{(p^nm)}$ has a normal p-integral basis over $K_{(p^\ell m)}$. The special case for $\ell=1$ and $m=1$ has been done by Komatsu([Kom94]). However, we shall develop it in more comprehensive way by utilizing (3.10) and Proposition 2.1 as in the previous section unlike Komatsu's method via class field theory. As a corollary we shall determine the existence of normal basis of the $\mathbb{Z}_p$-extension $K_\infty K_{(p^\ell)}/K_{(p^\ell)}$ for $\ell\geqslant 1$ where K_∞/K is a $\mathbb{Z}_p$-extension of K.

Let θ be as in (3.1) and set $\mathrm{irr}(\theta,\ K)=X^2+B_\theta X+C_\theta$. Then we can identify the Galois group $\Gamma=\mathrm{Gal}(K_{(p^{2(n-\ell)}m)}/K_{(p^\ell m)})$ with the group

$$\left\{\gamma=\left(\begin{smallmatrix} t-B_\theta s & -C_\theta s\\ s & t\end{smallmatrix}\right)\in\mathrm{GL}_2(\mathbb{Z}/p^{2(n-\ell)}m\mathbb{Z})\ :\ \gamma\equiv\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)\pmod{p^\ell m}\right\}/\left\{\pm\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)\right\}$$

by (3.10) and $\#\Gamma=[K_{(p^{2(n-\ell)}m)}:K_{(p^\ell m)}]=p^{2(2(n-\ell)-\ell)}$ by the formula (3.12).

Lemma 6.1. *There exists an element β_0 of $\mathrm{SL}_2(\mathbb{Z})$ satisfying the property*

$$\beta_0^{p^k}=\left(\begin{smallmatrix} * & *\\ p^{\ell+k}mq_k & *\end{smallmatrix}\right)\equiv\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)\pmod{p^{\ell+k}m}\qquad(0\leqslant k\leqslant 2(n-\ell)-\ell)\tag{6.1}$$

for some integers $q_k\not\equiv 0\pmod p$.

Proof. Consider an integral matrix $\beta=\left(\begin{smallmatrix}1+p^\ell mx-B_\theta p^\ell m & -C_\theta p^\ell m\\ p^\ell m & 1+p^\ell mx\end{smallmatrix}\right)$ for an undetermined integer x. Then the condition $\det(\beta)\equiv 1\pmod{p^{2(n-\ell)}m}$ is equivalent to

$$f(x)=p^\ell m^2x^2+(2m-B_\theta p^\ell m^2)x+C_\theta p^\ell m^2-B_\theta m\equiv 0\pmod{p^{2(n-\ell)-\ell}}.\tag{6.2}$$

Since $2m-B_\theta p^\ell m^2\not\equiv 0\pmod p$, the equation $f(x)\equiv 0\pmod p$ has a solution. Furthermore, since the derivative $f'(x)=2m-B_\theta p^\ell m^2\not\equiv 0\pmod p$, we have an integer solution $x=x_0$ of the congruence equation (6.2) by Hensel's lemma. Let β_0 be a preimage of $\left(\begin{smallmatrix}1+p^\ell mx_0-B_\theta p^\ell m & -C_\theta p^\ell m\\ p^\ell m & 1+p^\ell mx_0\end{smallmatrix}\right)$ via the natural surjection $\mathrm{SL}_2(\mathbb{Z})\to\mathrm{SL}_2(\mathbb{Z}/p^{2(n-\ell)}m\mathbb{Z})$. Then it is routine to check that β_0 satisfies the property (6.1). □

Set $\alpha=\left(\begin{smallmatrix}1+p^\ell m & 0\\ 0 & 1+p^\ell m\end{smallmatrix}\right)$ and $\beta=\beta_0$ in Lemma 6.1. Now that they have the order $p^{2(n-\ell)-\ell}$ in Γ and $\#\Gamma=p^{2(2(n-\ell)-\ell)}$, we derive

$$\Gamma=\langle\alpha\rangle\times\langle\beta\rangle.$$

as a direct product. And, we get

$$\mathrm{Gal}(K_{(p^{2(n-\ell)}m)}/K_{(p^n m)}) = \langle \alpha^{p^{n-\ell}} \rangle \times \langle \beta^{p^{n-\ell}} \rangle \tag{6.3}$$

by (3.10). Let us define a function

$$g(\tau) = \prod_{s=0}^{p^{n-2\ell}-1} g^{12m}_{(0,\frac{1}{p^{n-\ell}m})\beta^s}(\tau).$$

Since each factor $g^{12m}_{(0,\frac{1}{p^{n-\ell}m})\beta^s}(\tau)$ lies in $\mathcal{F}_{p^{2(n-\ell)}m}$ by Proposition 2.2, the singular value $g(\theta)$ belongs to $K_{(p^{2(n-\ell)}m)}$ by (3.9).

Lemma 6.2. *$K_{(p^n m)} = K_{(p^\ell m)}(\zeta_{p^n},\ g(\theta))$*

Proof. By the property (6.1) of β, $\beta^{p^{n-2\ell}}$ is of the form $\left(\begin{smallmatrix} 1+p^{n-\ell}mA & p^{n-\ell}mB \\ p^{n-\ell}mC & 1+p^{n-\ell}mD \end{smallmatrix}\right)$ for some integers A, B, C, D with $C \not\equiv 0 \pmod{p}$. We then deduce by (3.10) and (2.2) that

$$\begin{aligned} g(\theta)^\beta &= \prod_{s=0}^{p^{n-2\ell}-1} \left(g^{12m}_{(0,\frac{1}{p^{n-\ell}m})\beta^s}(\theta) \right)^\beta = \prod_{s=0}^{p^{n-2\ell}-1} g^{12m}_{(0,\frac{1}{p^{n-\ell}m})\beta^s\beta}(\theta) \quad \text{by Proposition 2.1(iii)} \\ &= \frac{g^{12m}_{(0,\frac{1}{p^{n-\ell}m})\beta^{p^{n-2\ell}}}(\theta)}{g^{12m}_{(0,\frac{1}{p^{n-\ell}m})}(\theta)} g(\theta) = \frac{g^{12m}_{(C,\frac{1}{p^{n-\ell}m}+D)}(\theta)}{g^{12m}_{(0,\frac{1}{p^{n-\ell}m})}(\theta)} g(\theta) = \zeta_{p^{n-\ell}}^{-6C} g(\theta) \quad \text{by Proposition 2.1(iv).} \end{aligned} \tag{6.4}$$

In particular, $g(\theta)^{p^{n-\ell}}$ is fixed by β and $g(\theta)$ is fixed by $\beta^{p^{n-\ell}}$ because β fixes $\zeta_{p^{n-\ell}}$ by (3.10) and (2.2). Note that $\alpha^{p^{n-2\ell}} = \left(\begin{smallmatrix} 1+p^{n-\ell}mE & 0 \\ 0 & 1+p^{n-\ell}mE \end{smallmatrix}\right)$ for some integer E. As an element of Γ we can decompose $\alpha^{p^{n-2\ell}}$ into

$$\alpha^{p^{n-2\ell}} = \alpha_1 \cdot \alpha_2 = \left(\begin{smallmatrix} 1 & 0 \\ 0 & (1+p^{n-\ell}mE)^2 \end{smallmatrix}\right) \left(\begin{smallmatrix} 1+p^{n-\ell}mE+p^{2(n-\ell)}mA' & p^{2(n-\ell)}mB' \\ p^{2(n-\ell)}mC' & E'+p^{2(n-\ell)}mD' \end{smallmatrix}\right)$$

for some integer A', B', C', D', E' such that $(1+p^{n-\ell}mE)E' \equiv 1 \pmod{p^{2(n-\ell)}m}$ and $\alpha_2 \in \mathrm{SL}_2(\mathbb{Z})$. Hence, we get by (3.10), (2.1), (2.2) and Proposition 2.1(iii) that

$$\begin{aligned} g(\theta)^{\alpha^{p^{n-2\ell}}} &= \prod_{s=0}^{p^{n-2\ell}-1} \left(g^{12m}_{(0,\frac{1}{p^{n-\ell}m})\beta^s}(\theta) \right)^{\alpha^{p^{n-2\ell}}} = \prod_{s=0}^{p^{n-2\ell}-1} \left(g^{12m}_{(0,\frac{1}{p^{n-\ell}m})}(\theta) \right)^{\beta^s \alpha^{p^{n-2\ell}}} \\ &= \prod_{s=0}^{p^{n-2\ell}-1} \left(g^{12m}_{(0,\frac{1}{p^{n-\ell}m})}(\theta) \right)^{\alpha^{p^{n-2\ell}}\beta^s} = \prod_{s=0}^{p^{n-2\ell}-1} \left(g^{12m}_{(0,\frac{1}{p^{n-\ell}m})}(\theta) \right)^{\alpha_1\alpha_2\beta^s} \\ &= \prod_{s=0}^{p^{n-2\ell}-1} \left(g^{12m}_{(0,\frac{1}{p^{n-\ell}m})}(\theta) \right)^{\alpha_2\beta^s} \quad \text{because } g^{12m}_{(0,\frac{1}{p^{n-\ell}m})}(\tau) \text{ has Fourier coefficients in } \mathbb{Q}(\zeta_{p^{n-\ell}m}) \\ &= \prod_{s=0}^{p^{n-2\ell}-1} \left(g^{12m}_{(0,\frac{1}{p^{n-\ell}m})\alpha_2}(\theta) \right)^{\beta^s} = \prod_{s=0}^{p^{n-2\ell}-1} \left(g^{12m}_{(p^{n-\ell}C',\frac{E'}{p^{n-\ell}m}+p^{n-\ell}D')}(\theta) \right)^{\beta^s} \\ &= \prod_{s=0}^{p^{n-2\ell}-1} \left(g^{12m}_{(0,\frac{1}{p^{n-\ell}m})}(\theta) \right)^{\beta^s} \quad \text{by the fact } E' \equiv 1 \pmod{p^{n-\ell}m} \text{ and Proposition 2.1(iv)} \\ &= \prod_{s=0}^{p^{n-2\ell}-1} g^{12m}_{(0,\frac{1}{p^{n-\ell}m})\beta^s}(\theta) = g(\theta). \end{aligned} \tag{6.5}$$

Observe that in particular, $g(\theta)$ is fixed by $\alpha^{p^{n-\ell}}$ and hence by $\langle\alpha^{p^{n-\ell}}\rangle \times \langle\beta^{p^{n-\ell}}\rangle$. Thus $g(\theta)$ belongs to $K_{(p^nm)}$ by (6.3).

On the other hand, we see from (3.10) that $\mathrm{Gal}(K_{(p^nm)}/K_{(p^\ell m)}) = \langle\alpha\rangle\times\langle\beta\rangle$ in $\mathrm{GL}_2(\mathbb{Z}/p^nm\mathbb{Z})/\{\pm\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)\}$ with α and β of order $p^{n-\ell}$. Suppose that $\alpha^A\beta^B$ fixes both ζ_{p^n} and $g(\theta)$ for some $0 \leqslant A,\ B < p^{n-\ell}$. Since $(\zeta_{p^n})^{\alpha^A\beta^B} = (\zeta_{p^n})^{\det(\alpha^A)} = \zeta_{p^n}^{(1+p^\ell m)^A}$ by (3.10), (2.1) and (2.2), we have $A = 0$. It then follows $B = 0$ from (6.4). Therefore we conclude that $K_{(p^nm)} = K_{(p^\ell m)}(\zeta_{p^n},\ g(\theta))$ by Galois theory. □

Now we are in the following situation:

$$\begin{tikzcd}
& K_{(p^nm)} = K_{(p^\ell m)}(\zeta_{p^n},\ g(\theta)) \arrow[dl, dash, "\text{cyclic of degree } p^{n-\ell}"'] \arrow[dr, dash, "\text{cyclic of degree } p^{n-\ell}"] & \\
K_{(p^\ell m)}(\zeta_{p^n}) \arrow[dr, dash, "\text{cyclic of degree } p^{n-\ell}"'] & & K_{(p^\ell m)}(g(\theta)) \arrow[dl, dash, "\text{cyclic of degree } p^{n-\ell}"] \\
& K_{(p^\ell m)} &
\end{tikzcd}$$

Here we see $K_{(p^\ell m)}(\zeta_{p^n}) \cap K_{(p^\ell m)}(g(\theta)) = K_{(p^\ell m)}$ by analyzing the actions of α and β in the proof of Lemma 6.2. Then we are ready to attain our aim by means of the following two lemmas:

Lemma 6.3. *Let L be a number field and F/L be a cyclic extension of a prime power degree $n = p^s$ which is unramified outside p.*

(i) When $\zeta_n \in L$, F has a normal p-integral basis over L if and only if $F = L(\sqrt[n]{\xi})$ for some $\xi \in \mathcal{O}_L[\frac{1}{p}]^*$.

(ii) When $\zeta_n \notin L$, F has a normal p-integral basis over L if and only if $F(\zeta_n)$ has a normal p-integral basis over $L(\zeta_n)$.

Proof. See [Gre92] Chapter 0 Proposition 6.5 and Chapter I Theorem 2.1. □

Lemma 6.4. *Let L be a number field and F_s/L be a cyclic extension which is unramfied outside p for $s = 1, 2$. If F_s has a normal p-integral basis over L for $s = 1,\ 2$ and $F_1 \cap F_2 = L$, then F_1F_2 has a normal p-integral basis over L.*

Proof. See [Kaw84] p. 227. □

Theorem 6.5. *Let $K(\neq \mathbb{Q}(\sqrt{-1}),\ \mathbb{Q}(\sqrt{-3}))$ be an imaginary quadratic field, $p \geqslant 5$ be a prime and $m \geqslant 1$ be an integer relatively prime to p. And, let n and ℓ be positive integers with $n \geqslant 2\ell$. Then $K_{(p^nm)}$ has a normal p-integral basis over $K_{(p^\ell m)}$.*

Proof. The extension $K_{(p^\ell m)}(\zeta_{p^n})/K_{(p^\ell m)}$ is cyclic of degree $p^{n-\ell}$ and is unramified outside p. We consider the extension $K_{(p^\ell m)}(\zeta_{p^n})/K_{(p^\ell m)}(\zeta_{p^{n-\ell}})$. It is also a cyclic extension of degree p^ℓ unramified outside p by considering the action of α on ζ_{p^n}. Since $K_{(p^\ell m)}(\zeta_{p^n}) = K_{(p^\ell m)}(\zeta_{p^{n-\ell}})(\sqrt[p^l]{\zeta_{p^{n-\ell}}})$, $K_{(p^\ell m)}(\zeta_{p^n})$ has a normal p-integral basis over $K_{(p^\ell m)}(\zeta_{p^{n-\ell}})$ by Lemma 6.3(i). If $n = 2\ell$, then $\zeta_{p^{n-\ell}} = \zeta_{p^\ell}$ and $K_{(p^\ell m)} = K_{(p^\ell m)}(\zeta_{p^{n-\ell}})$. If $n > 2\ell$, then $\zeta_{p^{n-\ell}} \notin K_{(p^\ell m)}$ and hence $K_{(p^\ell m)}(\zeta_{p^n})$ has a normal p-integral basis over $K_{(p^\ell m)}$ by Lemma 6.3(ii).

Next we look into the cyclic extension $K_{(p^\ell m)}(g(\theta))/K_{(p^\ell m)}$ of degree $p^{n-\ell}$ unramified outside p. Let us examine the extension $K_{(p^\ell m)}(\zeta_{p^{n-\ell}},\ g(\theta))/K_{(p^\ell m)}(\zeta_{p^{n-\ell}})$. Then we see that it is also a cyclic extension of degree $p^{n-\ell}$ unramified outside p by considering the action of β on $g(\theta)$. Note that we can rewrite it as $K_{(p^\ell m)}(\zeta_{p^{n-\ell}},\ g(\theta)) = K_{(p^\ell m)}(\zeta_{p^{n-\ell}})(\sqrt[p^{n-\ell}]{g(\theta)^{p^{n-\ell}}})$. On the other hand, we know by (3.10), (2.1) and (2.2) that $\mathrm{Gal}(K_{(p^{2(n-\ell)}m)}/K_{(p^\ell m)}(\zeta_{p^{n-\ell}})) = \langle\alpha^{p^{n-2\ell}}\rangle \times \langle\beta\rangle$. So $g(\theta)^{p^{n-\ell}}$ belongs to $K_{(p^\ell m)}(\zeta_{p^{n-\ell}})$ by (6.4) and (6.5). Moreover, it belongs to $\mathcal{O}_{K_{(p^\ell m)}(\zeta_{p^{n-\ell}})}[\frac{1}{p}]^*$ by Proposition 2.1(i) and (ii). Hence $K_{(p^\ell m)}(\zeta_{p^{n-\ell}},\ g(\theta))$ has a normal p-integral basis over $K_{(p^\ell m)}(\zeta_{p^{n-\ell}})$ by Lemma 6.3(i). If $n = 2\ell$, then $K_{(p^\ell m)} = K_{(p^\ell m)}(\zeta_{p^{n-\ell}})$. If $n > 2\ell$, then $\zeta_{p^{n-\ell}} \notin K_{(p^\ell m)}$ and hence $K_{(p^\ell m)}(g(\theta))$ has a normal p-integral basis over $K_{(p^\ell m)}$ by Lemma 6.3(ii).

Therefore the theorem follows from Lemma 6.4 because $K_{(p^\ell m)}(\zeta_{p^n}) \cap K_{(p^\ell m)}(g(\theta)) = K_{(p^\ell m)}$. □

Corollary 6.6. *Let $K(\neq \mathbb{Q}(\sqrt{-1}),\ \mathbb{Q}(\sqrt{-3}))$ be an imaginary quadratic field and $p \geqslant 5$ be a prime. Let K_∞ be any $\mathbb{Z}_p$-extension of K. Then the $\mathbb{Z}_p$-extension $K_\infty K_{(p^\ell)}/K_{(p^\ell)}$ has a normal basis over $K_{(p^\ell)}$ for $\ell \geqslant 1$.*

Proof. It is a direct consequence of Theorem 6.5 by the well-known fact that if an extension F/L of number fields has a normal p-integral basis over L, then so does F'/L for each intermediate field F'. □

References

Cha87 S-P. Chan, *Modular functions, elliptic functions and Galois module structure*, J. reine angew. Math. 375/376 (1987), 67-82

CY96 I. Chen and N. Yui, *Singular values of Thompson series*, Groups, difference sets, and the Monster (Columbus, OH, 1993), 255-326, Ohio State Univ. Math. Res. Inst. Publ., 4, Walter de Gruyter, Berlin, 1996.

CK B. Cho and J. K. Koo, *Construction of class fields over imaginary quadratic fields and applications*, Quart. J. Math., doi:10.1093/qmath/ham035.

Cox89 D. A. Cox, *Primes of the form $x^2 + ny^2$: Fermat, Class Field, and Complex Multiplication*, John Wiley & Sons, Inc., 1989.

CMS04 D. A. Cox, J. McKay and P. Stevenhagen, *Principal moduli and class fields*, Bull. London Math. Soc. 36 (2004), no. 1, 3-12.

FN91 V. Fleckinger and T. Nguyen-Quang-Do, *Bases normales unites et conjecture faible de Leopoldt*, Manuscr. Math. 71 (1991), no. 2, 183-195.

FK91 T. Fukuda and K. Komatsu, *Normal bases and λ-invariants of number fields*, Proc. Japan Acad. Ser. A Math. Sci. 67 (1991), no. 7, 243-245.

Gee99 A. Gee, *Class invariants by Shimura's reciprocity law*, J. Theor. Nombres Bordeaux 11 (1999), no. 1, 45-72.

Gre76 R. Greenberg, *On the Iwasawa invariants of totally real number fields*, American J. Math. 98 (1976), 263-284.

Gre92 C. Greither, *Cyclic Galois Extensions of Commutative Rings*, Lecture Notes in Mathematics, 1534, Springer-Verlag, 1992.

JKS H. Y. Jung, J. K. Koo and D. H. Shin, *Normal bases of the ray class fields over imaginary quadratic fields*, submitted.

JKS2 H. Y. Jung, J. K. Koo and D. H. Shin, *On some ray class invariants over imaginary quadratic fields*, submitted.

KY91 E. Kaltofen and N. Yui, *Explicit construction of the Hilbert class fields of imaginary quadratic fields by integer lattice reduction*, Number theory, 149-202, Springer, New York, 1991.

Kaw84 F. Kawamoto, *On normal integeral bases*, Tokyo J. Math. 7 (1984), 221-231.

Kom94 K. Komatsu, *Normal basis and Greenberg's conjecture*, Math. Ann. 300 (1994), no. 1, 157-163.

KS J. K. Koo and D. H. Shin, *On some arithmetic properties of Siegel functions*, Math. Zeit., DOI 10.1007/s00209-008-0456-9.

KL81 D. Kubert and S. Lang, *Modular Units*, Grundlehren der mathematischen Wissenschaften 244, Spinger-Verlag, 1981.

Lan87 S. Lang, *Elliptic Functions, 2nd edition*, Spinger-Verlag, 1987.

Mor88 F. Morain, *Implementation of the Atkin-Golwasser-Kilian primality testing algorithm*, draft, 1988.

Oka80 T. Okada, *Normal bases of class fields over Gauss' number field*, J. London Math. Soc. (2) 22 (1980), no. 2, 221-225.

Sch91 R. Schertz, *Galoismodulstruktur und elliptische Funktionen*, J. Number Theory 39 (1991), no. 3, 285-326.

Shi71 G. Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions*, Iwanami Shoten and Princeton University Press, 1971.

Sil94 J. H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Springer-verlag, 1994.

Tay85 M. J. Taylor, *Relative Galois module structure of rings of integers and elliptic functions. II*, Ann. of Math. (2) 121 (1985), no. 3, 519-535.

Was96 L. C. Washington, *Introduction to Cyclotomic Fields, 2nd edition*, Spinger, 1996.

Ho Yun Jung DOSAL@math.kaist.ac.kr
Department of Mathematical Sciences, KAIST
Current address: Daejeon 373-1, Korea

Ja Kyung Koo jkkoo@math.kaist.ac.kr
Department of Mathematical Sciences, KAIST
Current address: Daejeon 373-1, Korea

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