ON SOME RING CLASS INVARIANTS OVER IMAGINARY QUADRATIC FIELDS (II)

ICK SUN EUM, JA KYUNG KOO, AND DONG HWA SHIN

Abstract. Let K be an imaginary quadratic field. We show by adopting Schertz's argument with the Siegel-Ramachandra invariant([14]) that singular values of certain quotients of the Δ-function generate ring class fields over K(Theorems 4.2, 5.4 and Remark 5.5).

1. Introduction

In number theory ring class fields over imaginary quadratic fields, more precisely, primitive generators of ring class fields as real algebraic integers 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 the imaginary quadratic field $K=\mathbb{Q}(\sqrt{-n})$. If p is an odd prime not dividing n, then we have the following assertion:

$$\begin{aligned} & p=x^2+ny^2 \text{ is solvable for some integers } x \text{ and } y\\ \Longleftrightarrow\ & \text{the Legendre symbol } \left(\tfrac{-n}{p}\right)=1 \text{ and } f_n(X)\equiv 0 \pmod{p} \text{ has an integer solution}\end{aligned}$$

where $f_n(X)$ is the minimal polynomial of a real algebraic integer α for which $H_\mathcal{O}=K(\alpha)$([4]).

Given an imaginary quadratic field K with the ring of integer $\mathcal{O}_K=\mathbb{Z}[\theta]$ such that $\theta\in\mathfrak{H}$(=the complex upper half plane), let $\mathcal{O}=[N\theta,\ 1]$ be the order of conductor $N(\geq 1)$ in K. Then we know a classical result from the main theorem of complex multiplication that the j-invariant $j(\mathcal{O})=j(N\theta)$ generates the ring class field $H_\mathcal{O}$ over K([12] or [15]). Moreover, we have an algorithm of finding the minimal polynomial(=class polynomial) of such generator $j(\mathcal{O})$([4]) whose coefficients are too gigantic to handle for practical use.

Thus, unlike the classical case Chen-Yui([1]) 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 $\Gamma_0^\dagger(N)$, where $\Gamma_0(N)=\{\gamma\in\mathrm{SL}_2(\mathbb{Z}):\gamma\equiv\left(\begin{smallmatrix}*&*\\0&*\end{smallmatrix}\right)\pmod{N}\}$ and $\Gamma_0^\dagger(N)=\left\langle\Gamma_0(N),\left(\begin{smallmatrix}0&-1/\sqrt{N}\\\sqrt{N}&0\end{smallmatrix}\right)\right\rangle$ in $\mathrm{SL}_2(\mathbb{R})$. In like manner, Cox-Mckay-Stevenhagen([5]) showed that certain sigular value of a Hauptmodul for $\Gamma_0(N)$ or $\Gamma_0^\dagger(N)$ with rational Fourier coefficients generates $H_\mathcal{O}$ over K. And, Cho-Koo([2]) recently revisited and extended these results by using the theory of Shimura's canonical models and his reciprocity law.

On the other hand, Ramachandra showed in [13] that arbitrary finite abelian extension of an imaginary quadratic field K can be generated over K by a theoretically beautiful elliptic unit, but his invariant involves too complicated product of high powers of singular values of the Klein forms and singular values of the Δ-function to use in practice. This motivates our work of finding simpler ring class invariants in terms of the Siegel-Ramachandra invariant as Lang pointed out in his book([12] p.292) in case of ray class fields.

2000 *Mathematics Subject Classification.* 11F11, 11G15, 11R37.

Key words and phrases. modular forms and functions, ring class fields, Siegel functions.

This research was supported by Basic Science Research Program through the National Research Foundation of Korea funded by the Ministry of Education, Science and Technology (2009-0063182).

Koo-Shin established in [9] that if $K \neq \mathbb{Q}(\sqrt{-1}),\ \mathbb{Q}(\sqrt{-3})$ and p is a prime which is inert or ramified in $K/\mathbb{Q}$, then the real algebraic integer

$$p^{12}\frac{\Delta(p^e\theta)}{\Delta(p^{e-1}\theta)}$$

generates the ring class field $H_\mathcal{O}$ of the order $\mathcal{O}=[p^e\theta,\ 1](e\geq 1)$ where

$$\Delta(\tau)=(2\pi i)^{12}q_\tau\prod_{n=1}^{\infty}(1-q_\tau^n)^{24}\quad(\tau\in\mathfrak{H}) \tag{1.1}$$

is the *discriminant function* (or, Δ-function). And, this value is in fact certain root of the norm of the Siegel-Ramachandra invariant $g_\mathfrak{f}(C_0)$ with $\mathfrak{f}=p^e\mathcal{O}_K$(see Section 2) from the ray class field $K_\mathfrak{f}$ modulo $\mathfrak{f}$ to $H_\mathcal{O}$.

This paper is a continuation of our previous work. More precisely, for any pair $(r_1,\ r_2)\in\mathbb{Q}^2\setminus\mathbb{Z}^2$ we first define a *Siegel function* $g_{(r_1,\ r_2)}(\tau)$ by the following Fourier expansion

$$g_{(r_1,\ r_2)}(\tau)=-q_\tau^{\frac{1}{2}\mathbf{B}_2(r_1)}e^{\pi i r_2(r_1-1)}(1-q_z)\prod_{n=1}^{\infty}(1-q_\tau^n q_z)(1-q_\tau^n q_z^{-1})\quad(\tau\in\mathfrak{H}) \tag{1.2}$$

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 $z=r_1\tau+r_2$. As singular values of Siegel functions we shall define the Siegel-Ramachandra invariants in Section 2. And, motivated from the idea of Schertz([14]) we shall determine certain class fields over K generated by norms of the Siegel-Ramachandra invariants(Theorem 2.7). Furthermore, in case of ring class field, the product formulas (1.1), (1.2) and Theorem 2.7 enable us to express the norms as singular values of certain quotients of the Δ-function(Theorem 4.2). For example, let

$$N=\prod_{k=1}^{n}p_k^{e_k}$$

be a product of odd primes p_k which are inert or ramified in $K/\mathbb{Q}$ and we further assume that

$$e_k+1>\frac{2}{r_k}\quad\text{for all } k=1,\cdots,n\quad\text{and}\quad\begin{cases}\gcd(p_1,\ w_K)=1 & \text{if } n=1\\ \gcd\left(\prod_{k=1}^{n}p_k,\ \prod_{k=1}^{n}(p_k^{\frac{2}{r_k}}-1)\right)=1 & \text{if } n\geq 2,\end{cases}$$

where r_k is the ramification index of p_k in $K/\mathbb{Q}$ and w_K is the number of roots of unity in K. Then certain quotient of singular values $\Delta\left(\frac{N}{N_S}\theta\right)$, where N_S are the products of p_k's, becomes a generator of the ring class field of the order of conductor N over K(Remark 4.3). This would be an extension of the result in [9].

In Section 4, Theorem 4.2 heavily depends on Lemma 2.5 which requires the assumption (2.3). In Section 5, however, we shall develop certain lemma which substitutes for Lemma 2.5 in order to release from the assumption (2.3) to some extent(Lemma 5.3 and Remark 5.5). For example, let $K\neq\mathbb{Q}(\sqrt{-1}),\ \mathbb{Q}(\sqrt{-3})$ and

$$N=\prod_{a=1}^{A}s_a^{u_a}\prod_{b=1}^{B}q_b^{v_b}\prod_{c=1}^{C}r_c^{w_c}$$

be the prime factorization of N, where each s_a (respectively, q_b and r_c) splits completely (respectively, is inert and ramified) in $K/\mathbb{Q}$ and $A,\ B,\ C \geq 0$, and assume

$$4\sum_{a=1}^{A}\frac{1}{(s_a-1)s_a^{u_a-1}}+2\sum_{b=1}^{B}\frac{1}{(q_b+1)q_b^{v_b-1}}+2\sum_{c=1}^{C}\frac{1}{r_c^{w_c}}<1.$$

Then one can also apply Theorem 4.2 without assuming (2.3)(Theorem 5.4, Remark 5.5).

And, by making use of our simple invariant developed in Theorem 4.2 we present three examples(Examples 4.4, 4.5 and 5.6).

2. Primitive generators of class fields

In this section we investigate some class fields over imaginary quadratic fields generated by norms of the Siegel-Ramachandra invariants.

For a given imaginary quadratic field K we let

$$\begin{array}{rcl} d_K & : & \text{the discriminant of } K \\ \mathfrak{d}_K & : & \text{the different of } K/\mathbb{Q} \\ \mathcal{O}_K & : & \text{the ring of integers of } K \\ w_K & : & \text{the number of root of unity in } K \\ I_K & : & \text{the group of fractional ideals of } K \\ P_K & : & \text{the subgroup of } I_K \text{ consisting of principal ideals of } K. \end{array}$$

And, for a nonzero integral ideal $\mathfrak{f}$ of K we set

$$\begin{array}{rcl} I_K(\mathfrak{f}) & : & \text{the subgroup of } I_K \text{ consisting of ideals relatively prime to } \mathfrak{f} \\ P_{K,1}(\mathfrak{f}) & : & \text{the subgroup of } I_K(\mathfrak{f})\cap P_K \text{ generated by the principal ideals } \alpha\mathcal{O}_K \\ & & \text{for which } \alpha\in\mathcal{O}_K \text{ satisfies } \alpha\equiv 1 \pmod{\mathfrak{f}} \\ \mathrm{Cl}(\mathfrak{f}) & : & \text{the ray class group (modulo } \mathfrak{f}),\ \text{namely } I_K(\mathfrak{f})/P_{K,1}(\mathfrak{f}) \\ C_0 & : & \text{the unit class of } \mathrm{Cl}(\mathfrak{f}) \\ w(\mathfrak{f}) & : & \text{the number of roots of unity in } K \text{ which are} \equiv 1 \pmod{\mathfrak{f}} \\ N(\mathfrak{f}) & : & \text{the smallest positive integer in } \mathfrak{f}. \end{array}$$

By the *ray class field* $K_\mathfrak{f}$ *modulo* $\mathfrak{f}$ *of* K we mean a finite abelan extension of K whose Galois group is isomorphic to $\mathrm{Cl}(\mathfrak{f})$ via the Artin map σ, namely

$$\sigma=\left(\frac{K_\mathfrak{f}/K}{\cdot}\right)\ :\ \mathrm{Cl}(\mathfrak{f})\longrightarrow \mathrm{Gal}(K_\mathfrak{f}/K).$$

In particular, if $\mathfrak{f}=\mathcal{O}_K$, we denote $K_\mathfrak{f}$ by H and call it the *Hilbert class field of* K. Then by definition and characterization of ray class field([12] p.109 or [3] Proposition 3.2.3) we have a short exact sequence

$$1\longrightarrow \pi_\mathfrak{f}(\mathcal{O}_K)^*/\pi_\mathfrak{f}(\mathcal{O}_K^*)\xrightarrow{\Phi_\mathfrak{f}}\mathrm{Cl}(\mathfrak{f})\longrightarrow \mathrm{Cl}(\mathcal{O}_K)\longrightarrow 1 \tag{2.1}$$

where

$$\pi_\mathfrak{f}\ :\ \mathcal{O}_K\longrightarrow \mathcal{O}_K/\mathfrak{f}$$

is the natural surjection and $\Phi_\mathfrak{f}$ is induced by the homomorphism

$$\begin{array}{rcl} \widetilde{\Phi}_\mathfrak{f}\ :\ \pi_\mathfrak{f}(\mathcal{O}_K)^* & \longrightarrow & \mathrm{Cl}(\mathfrak{f}) \\ \pi_\mathfrak{f}(x) & \mapsto & [x\mathcal{O}_K]\ \text{the class containing } x\mathcal{O}_K \end{array}$$

whose kernel is $\pi_{\mathfrak{f}}(\mathcal{O}_K^*)$. Let χ be a character of $\mathrm{Cl}(\mathfrak{f})$. We then denote by $\mathfrak{f}_\chi$ the conductor of χ, namely

$$\mathfrak{f}_\chi = \gcd\Big(\mathfrak{g}\ :\ \chi = \psi \circ \big(\mathrm{Cl}(\mathfrak{f}) \to \mathrm{Cl}(\mathfrak{g})\big) \text{ for some character } \psi \text{ of } \mathrm{Cl}(\mathfrak{g})\Big),$$

and let χ_0 be the proper character of $\mathrm{Cl}(\mathfrak{f}_\chi)$ corresponding to χ. Similarly, if χ' is any character of $\pi_{\mathfrak{f}}(\mathcal{O}_K)^*$, then the conductor $\mathfrak{f}_{\chi'}$ of χ' is defined by

$$\mathfrak{f}_{\chi'} = \gcd\Big(\mathfrak{g}\ :\ \chi' = \psi' \circ \big(\pi_{\mathfrak{f}}(\mathcal{O}_K)^* \to \pi_{\mathfrak{g}}(\mathcal{O}_K)^*\big) \text{ for some character } \psi' \text{ of } \pi_{\mathfrak{g}}(\mathcal{O}_K)^*\Big).$$

Now, for a character χ of $\mathrm{Cl}(\mathfrak{f})$ we define a character $\widetilde{\chi}$ of $\pi_{\mathfrak{f}}(\mathcal{O}_K)^*$ by

$$\widetilde{\chi} = \chi \circ \widetilde{\Phi}_{\mathfrak{f}}.$$

And, if

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

then from the Chinese remainder theorem we have an isomorphism

$$\iota : \prod_{k=1}^{n} \pi_{\mathfrak{p}_k^{e_k}}(\mathcal{O}_K)^* \xrightarrow{\sim} \pi_{\mathfrak{f}}(\mathcal{O}_K)^*,$$

and natural injections and surjections

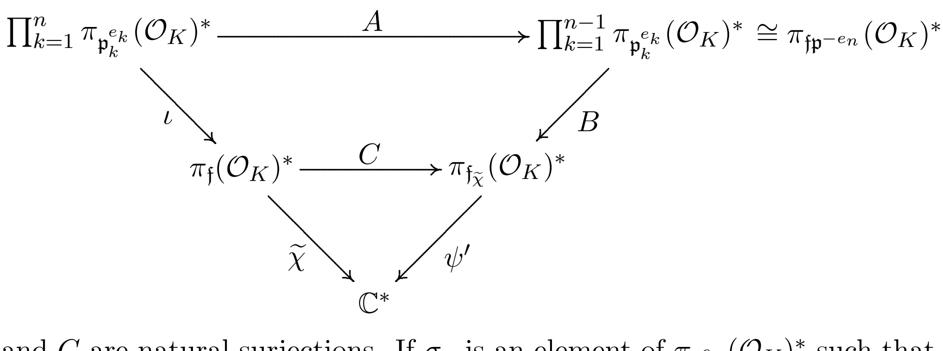
$$\iota_k\ :\ \pi_{\mathfrak{p}_k^{e_k}}(\mathcal{O}_K)^* \hookrightarrow \prod_{\ell=1}^{n} \pi_{\mathfrak{p}_\ell^{e_\ell}}(\mathcal{O}_K)^* \quad\text{and}\quad \upsilon_k\ :\ \prod_{\ell=1}^{n} \pi_{\mathfrak{p}_\ell^{e_\ell}}(\mathcal{O}_K)^* \to \pi_{\mathfrak{p}_k^{e_k}}(\mathcal{O}_K)^* \quad (k = 1, \cdots, n),$$

respectively. Furthermore, we consider characters $\widetilde{\chi}_k$ of $\pi_{\mathfrak{p}_k^{e_k}}(\mathcal{O}_K)^*$ defined by

$$\widetilde{\chi}_k = \widetilde{\chi} \circ \iota \circ \iota_k \quad (k = 1, \cdots, n).$$

Lemma 2.1. (i) $\mathfrak{f}_{\widetilde{\chi}} = \mathfrak{f}_\chi$.
(ii) $\widetilde{\chi} \circ \iota = \prod_{k=1}^{n} \widetilde{\chi}_k \circ \upsilon_k$.
(iii) *If* $\widetilde{\chi}_k \neq 1$, *then* $\mathfrak{p}_k \mid \mathfrak{f}_{\widetilde{\chi}}$.

Proof. (i) and (ii) are immediate by definitions of conductors and the maps $\widetilde{\chi}$, $\widetilde{\chi}_k$, ι and υ_k.
(iii) Without loss of generality we may assume $\widetilde{\chi}_n \neq 1$. Suppose on the contrary $\mathfrak{p}_n \nmid \mathfrak{f}_{\widetilde{\chi}}$. Then by definition of $\mathfrak{f}_{\widetilde{\chi}}$ there is a character ψ' of $\mathrm{Cl}(\mathfrak{f}_{\widetilde{\chi}})$ which makes the following diagram commute:



where A, B and C are natural surjections. If σ_n is an element of $\pi_{\mathfrak{p}_n^{e_n}}(\mathcal{O}_K)^*$ such that $\widetilde{\chi}_n(\sigma_n) \neq 1$, then

$$\begin{aligned} 1 &\neq \widetilde{\chi}_n(\sigma_n) = \widetilde{\chi} \circ \iota \circ \iota_n(\sigma_n) = \widetilde{\chi} \circ \iota(1, \cdots, 1, \sigma_n) \\ &= (\psi' \circ C) \circ \iota(1, \cdots, 1, \sigma_n) = \psi' \circ B \circ A(1, \cdots, 1, \sigma_n) = \psi' \circ B(1, \cdots, 1) = 1, \end{aligned}$$

which renders a contradiction. Therefore, $\mathfrak{p}_n \mid \mathfrak{f}_{\widetilde{\chi}}$. □

If $\mathfrak{f} \neq \mathcal{O}_K$ and $C \in \mathrm{Cl}(\mathfrak{f})$, we take an integral ideal $\mathfrak{c}$ in C so that $\mathfrak{f}\mathfrak{c}^{-1} = [z_1,\ z_2]$ with $z = \frac{z_1}{z_2} \in \mathfrak{H}$. Then, we define the *Siegel-Ramachandra invariant* by

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

where $a,\ b \in \mathbb{Z}$ such that $1 = \frac{a}{N(\mathfrak{f})}z_1 + \frac{b}{N(\mathfrak{f})}z_2$. This value depends only on the class C and belongs to the ray class field $K_\mathfrak{f}$. And, we have a well-known transformation formula

$$g_\mathfrak{f}(C_1)^{\sigma(C_2)} = g_\mathfrak{f}(C_1C_2) \tag{2.2}$$

for $C_1,\ C_2 \in \mathrm{Cl}(\mathfrak{f})$([10] Chapter 11).

For a nontrivial character χ of $\mathrm{Cl}(\mathfrak{f})$ with $\mathfrak{f} \neq \mathcal{O}_K$ we define the *Stickelberger element* as

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

and consider the L-function

$$L_\mathfrak{f}(s,\ \chi) = \sum_{\mathfrak{a} \neq 0\ :\ \text{integral ideals of } K} \frac{\chi(\mathfrak{a})}{\mathbf{N}_{K/\mathbb{Q}}(\mathfrak{a})^s} \quad (s \in \mathbb{C}).$$

Then, from the second Kronecker limit formula we get the following proposition.

Proposition 2.2. *If $\mathfrak{f}_\chi \neq \mathcal{O}_K$, then*

$$\prod_{\mathfrak{p} \mid \mathfrak{f},\ \mathfrak{p} \nmid \mathfrak{f}_\chi} \big(1 - \overline{\chi}_0(\mathfrak{p})\big) L_{\mathfrak{f}_\chi}(1,\ \chi_0) = \frac{\pi}{3w(\mathfrak{f})N(\mathfrak{f})\tau(\overline{\chi}_0)\sqrt{-d_K}} S_\mathfrak{f}(\overline{\chi},\ g_\mathfrak{f})$$

where

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

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

Proof. See [12] Chapter 22 Theorem 2 and [10] Chapter 11 Theorem 2.1. □

Remark 2.3. (i) The product factor $\prod_{\mathfrak{p} \mid \mathfrak{f},\ \mathfrak{p} \nmid \mathfrak{f}_\chi} \big(1 - \overline{\chi}_0(\mathfrak{p})\big)$ is called the *Euler factor of* χ. If there is no such $\mathfrak{p}$ with $\mathfrak{p} \mid \mathfrak{f}$ and $\mathfrak{p} \nmid \mathfrak{f}_\chi$, then it is understood to be 1.
(ii) As is well-known([7] Chapter IV Proposition 5.7) $L_{\mathfrak{f}_\chi}(1,\ \chi_0) \neq 0$.

Lemma 2.4. *Let $A \subsetneq B$ be finite abelian groups, $b \in B \setminus A$ and χ be a character of A. Let m be the order of the coset bA in the quotient group B/A. Then we can extend χ to a character ψ of B such that $\psi(b)$ is any m-th root of $\chi(b^m)$.*

Proof. It suffices to prove the case $B = \langle A,\ b\rangle$. Let ζ be any m-th root of $\chi(b^m)$. Define a map

$$\begin{aligned} \psi\ :\ \langle A,\ b\rangle &\longrightarrow \mathbb{C}^* \\ ab^k &\mapsto \chi(a)\zeta^k \quad (a \in A). \end{aligned}$$

Using the fact $\zeta^m = \chi(b^m)$ one can readily show that ψ is a (well-defined) character of $\langle A,\ b\rangle$ which extends χ and also satisfies $\psi(b) = \zeta$. □

Lemma 2.5. *Let $L(\neq K)$ be a finite abelian extension of K contained in some ray class field $K_\mathfrak{f}$ modulo*

$$\mathfrak{f}(\neq \mathcal{O}_K)=\prod_{k=1}^{n}\mathfrak{p}_k^{e_k}.$$

For an intermediate field F between K and $K_\mathfrak{f}$ we denote by $\mathrm{Cl}(K_\mathfrak{f}/F)$ the subgroup of $\mathrm{Cl}(\mathfrak{f})$ corresponding to $\mathrm{Gal}(K_\mathfrak{f}/F)$ via the Artin map. Let

$$\widehat{\varepsilon}_k=\#\ \mathrm{Ker}\Big(\textit{the natural projection } \widehat{\rho}_k\ :\ \pi_\mathfrak{f}(\mathcal{O}_K)^*/\pi_\mathfrak{f}(\mathcal{O}_K^*)\longrightarrow \pi_{\mathfrak{f}\mathfrak{p}_k^{-e_k}}(\mathcal{O}_K)^*/\pi_{\mathfrak{f}\mathfrak{p}_k^{-e_k}}(\mathcal{O}_K^*)\Big)$$

and

$$\varepsilon_k=\#\ \mathrm{Ker}\Big(\textit{the natural projection } \rho_k\ :\ \pi_\mathfrak{f}(\mathcal{O}_K)^*/\pi_\mathfrak{f}(\mathcal{O}_K^*)\longrightarrow \pi_{\mathfrak{p}_k^{e_k}}(\mathcal{O}_K)^*/\pi_{\mathfrak{p}_k^{e_k}}(\mathcal{O}_K^*)\Big)$$

for each $k=1,\cdots,n$. Assume that

$$\begin{array}{l}\textit{for each } k=1,\cdots,n \textit{ there is an odd prime } \nu_k \textit{ such that}\\ \nu_k\nmid\varepsilon_k \textit{ and } \mathrm{ord}_{\nu_k}(\widehat{\varepsilon}_k)>\mathrm{ord}_{\nu_k}\big(\#\ \mathrm{Cl}(K_\mathfrak{f}/L)\big).\end{array}\tag{2.3}$$

If D is a class in $\mathrm{Cl}(\mathfrak{f})\setminus\mathrm{Cl}(K_\mathfrak{f}/L)$, then there exists a character χ of $\mathrm{Cl}(\mathfrak{f})$ such that

$$\chi|_{\mathrm{Cl}(K_\mathfrak{f}/L)}=1,\quad \chi(D)\neq 1\quad \textit{and}\quad \mathfrak{p}_k\mid\mathfrak{f}_\chi\quad \textit{for all } k=1,\cdots,n.\tag{2.4}$$

Proof. Since $D\in\mathrm{Cl}(\mathfrak{f})\setminus\mathrm{Cl}(K_\mathfrak{f}/L)$, there is a character χ of $\mathrm{Cl}(\mathfrak{f})$ such that

$$\chi|_{\mathrm{Cl}(K_\mathfrak{f}/L)}=1\quad\text{and}\quad\chi(D)\neq 1$$

by Lemma 2.4. Let $\widetilde{\chi}_k$ $(k=1,\cdots,n)$ be the character of $\pi_{\mathfrak{p}_k^{e_k}}(\mathcal{O}_K)^*$ induced from χ as in Lemma 2.1.

Suppose $\widetilde{\chi}_k=1$ for some k. Let ν_k be a prime number in the assumption (2.3) and S be a Sylow ν_k-subgroup of $\Phi_\mathfrak{f}\big(\mathrm{Ker}(\widehat{\rho}_k)\big)$. Then $\mathrm{Cl}(K_\mathfrak{f}/L)$ does not contain S by (2.3). Hence we can take an element C in $S\setminus\mathrm{Cl}(K_\mathfrak{f}/L)$ whose order is a power of ν_k. Now we extend the trivial character of $\mathrm{Cl}(K_\mathfrak{f}/L)$ to a character ψ' of $\mathrm{Cl}(\mathfrak{f})$ so that $\psi'(C)=\zeta_{\nu_k}=e^{\frac{2\pi i}{\nu_k}}$ by Lemma 2.4, because the order of the coset $C\mathrm{Cl}(K_\mathfrak{f}/L)$ in the quotient group $\mathrm{Cl}(\mathfrak{f})/\mathrm{Cl}(K_\mathfrak{f}/L)$ is also a power of ν_k. Define a character ψ of $\mathrm{Cl}(\mathfrak{f})$ by

$$\psi=\begin{cases}\psi'^{\varepsilon_k} & \text{if } \chi(D)\psi'^{\varepsilon_k}(D)\neq 1\\ \psi'^{2\varepsilon_k} & \text{otherwise.}\end{cases}$$

Then we achieve

$$(\chi\psi)|_{\mathrm{Cl}(K_\mathfrak{f}/L)}=1\quad\text{and}\quad(\chi\psi)(D)=\chi(D)\psi(D)\neq 1.$$

Furthermore, since $\Big(\iota\circ\iota_\ell\big(\pi_{\mathfrak{p}_\ell^{e_\ell}}(\mathcal{O}_K)^*\big)\Big)\pi_\mathfrak{f}(\mathcal{O}_K^*)/\pi_\mathfrak{f}(\mathcal{O}_K^*)$ is a subgroup of $\mathrm{Ker}(\rho_k)$ for $\ell\neq k$(see the diagram (2.5) below), we derive that

$$\begin{aligned}\widetilde{\psi}_\ell\big(\pi_{\mathfrak{p}_\ell^{e_\ell}}(\mathcal{O}_K)^*\big) &= \psi\circ\widetilde{\Phi}_\mathfrak{f}\circ\iota\circ\iota_\ell\big(\pi_{\mathfrak{p}_\ell^{e_\ell}}(\mathcal{O}_K)^*\big)\quad\text{by definition of } \widetilde{\psi}_\ell \text{ in Lemma 2.1}\\ &\subseteq \psi\Big(\Phi_\mathfrak{f}\big(\mathrm{Ker}(\rho_k)\big)\Big)\\ &= \psi'^{\varepsilon_k}\Big(\Phi_\mathfrak{f}\big(\mathrm{Ker}(\rho_k)\big)\Big)\ \text{or}\ \psi'^{2\varepsilon_k}\Big(\Phi_\mathfrak{f}\big(\mathrm{Ker}(\rho_k)\big)\Big)=1,\end{aligned}$$

which yields

$$\widetilde{\psi}_\ell=1\quad\text{and}\quad\widetilde{(\chi\psi)}_\ell=\widetilde{\chi}_\ell\widetilde{\psi}_\ell=\widetilde{\chi}_\ell\quad\text{for } \ell\neq k.$$

On the other hand, since $C \in \Phi_\mathfrak{f}\big(\mathrm{Ker}(\widehat{\rho}_k)\big) \subseteq \mathrm{Im}(\Phi_\mathfrak{f})$, we can take an element c of $\pi_\mathfrak{f}(\mathcal{O}_K)^*$ so that $\widetilde{\Phi}_\mathfrak{f}(c) = C$. Thus we get that

$$\widetilde{\psi}(c) = \psi \circ \widetilde{\Phi}_\mathfrak{f}(c) = \psi(C) = \psi'^{\varepsilon_k}(C) \text{ or } \psi'^{2\varepsilon_k}(C) = \zeta_{\nu_k}^{\varepsilon_k} \text{ or } \zeta_{\nu_k}^{2\varepsilon_k} \neq 1,$$

which shows $\widetilde{\psi} \neq 1$, and hence $\widetilde{\psi}_k \neq 1$ by the fact $\widetilde{\psi}_\ell = 1$ for $\ell \neq k$ and Lemma 2.1(ii). Therefore we obtain

$$(\widetilde{\chi\psi})_k = \widetilde{\chi}_k \widetilde{\psi}_k = \widetilde{\psi}_k \neq 1.$$

Now, we replace χ by $\chi\psi$ and repeat the above process for finitely many $\ell(\neq k)$ such that $\widetilde{\chi}_\ell = 1$. After this procedure, we finally establish a character χ of $\mathrm{Cl}(\mathfrak{f})$ which satisfies

$$\chi|_{\mathrm{Cl}(K_\mathfrak{f}/L)} = 1, \quad \chi(D) \neq 1 \quad \text{and} \quad \widetilde{\chi}_k \neq 1 \quad \text{for all } k = 1, \cdots, n.$$

And we derive by Lemma 2.1 that $\mathfrak{p}_k \mid \mathfrak{f}_\chi$ for all $k = 1, \cdots, n$. This proves the lemma. □

Remark 2.6. From the commutative diagram of exact sequences

$$\begin{array}{ccccccccc}
1 & \longrightarrow & \pi_\mathfrak{f}(\mathcal{O}_K)^*/\pi_\mathfrak{f}(\mathcal{O}_K^*) & \xrightarrow{\Phi_\mathfrak{f}} & \mathrm{Cl}(\mathfrak{f}) & \longrightarrow & \mathrm{Cl}(\mathcal{O}_K) & \longrightarrow & 1 \\
 & & \downarrow{\scriptstyle \widehat{\rho}_k} & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & \pi_{\mathfrak{f}\mathfrak{p}_k^{-e_k}}(\mathcal{O}_K)^*/\pi_{\mathfrak{f}\mathfrak{p}_k^{-e_k}}(\mathcal{O}_K^*) & \xrightarrow{\Phi_{\mathfrak{f}\mathfrak{p}_k^{-e_k}}} & \mathrm{Cl}(\mathfrak{f}\mathfrak{p}_k^{-e_k}) & \longrightarrow & \mathrm{Cl}(\mathcal{O}_K) & \longrightarrow & 1
\end{array}$$

where vertical maps are natural projections, one can readily obtain

$$\mathrm{Cl}(\mathfrak{f})/\Phi_\mathfrak{f}\big(\mathrm{Ker}(\widehat{\rho}_k)\big) \cong \mathrm{Cl}(\mathfrak{f}\mathfrak{p}_k^{-e_k}) \cong \mathrm{Cl}(\mathfrak{f})/\mathrm{Cl}(K_\mathfrak{f}/K_{\mathfrak{f}\mathfrak{p}_k^{-e_k}}).$$

Hence we have

$$\widehat{\varepsilon}_k = \#\ \mathrm{Ker}(\widehat{\rho}_k) = \#\ \Phi_\mathfrak{f}\big(\mathrm{Ker}(\widehat{\rho}_k)\big) = [K_\mathfrak{f} : K_{\mathfrak{f}\mathfrak{p}_k^{-e_k}}] = \frac{\varphi(\mathfrak{p}_k^{e_k})w(\mathfrak{f})}{w(\mathfrak{f}\mathfrak{p}_k^{-e_k})}$$

by using Lemma 3.4(ii), which will be used in the next section. Similarly, again from the commutative diagram

$$\begin{array}{ccccccccc}
1 & \longrightarrow & \pi_\mathfrak{f}(\mathcal{O}_K)^*/\pi_\mathfrak{f}(\mathcal{O}_K^*) & \xrightarrow{\Phi_\mathfrak{f}} & \mathrm{Cl}(\mathfrak{f}) & \longrightarrow & \mathrm{Cl}(\mathcal{O}_K) & \longrightarrow & 1 \\
 & & \downarrow{\scriptstyle \wr} & & & & & & \\
 & & \prod_{\ell=1}^n \pi_{\mathfrak{p}_\ell^{e_\ell}}(\mathcal{O}_K)^*/\big\{ \prod_{\ell=1}^n \pi_{\mathfrak{p}_\ell^{e_\ell}}(x) \ : \ x \in \mathcal{O}_K^* \big\} & & \big\downarrow & & \big\downarrow & & \\
 & & \downarrow{\scriptstyle \rho_k} & & & & & & \\
1 & \longrightarrow & \pi_{\mathfrak{p}_k^{e_k}}(\mathcal{O}_K)^*/\pi_{\mathfrak{p}_k^{e_k}}(\mathcal{O}_K^*) & \xrightarrow{\Phi_{\mathfrak{p}_k^{e_k}}} & \mathrm{Cl}(\mathfrak{p}_k^{e_k}) & \longrightarrow & \mathrm{Cl}(\mathcal{O}_K) & \longrightarrow & 1
\end{array} \tag{2.5}$$

we come up with

$$\varepsilon_k = \#\ \mathrm{Ker}(\rho_k) = \#\ \Phi_\mathfrak{f}\big(\mathrm{Ker}(\rho_k)\big) = [K_\mathfrak{f} : K_{\mathfrak{p}_k^{e_k}}] = \frac{\prod_{\ell=1}^n \varphi(\mathfrak{p}_\ell^{e_\ell})w(\mathfrak{f})}{\varphi(\mathfrak{p}_k^{e_k})w(\mathfrak{p}_k^{e_k})}.$$

Theorem 2.7. *Let L be a field in Lemma 2.5 which satisfies the assumption (2.3). Then the singular value*

$$\varepsilon = \mathbf{N}_{K_{\mathfrak{f}}/L}\Big(g_{\mathfrak{f}}(C_0)\Big)$$

generates L over K.

Proof. Let $F = K(\varepsilon)$ as a subfield of L. Suppose that F is properly contained in L. Then for a class D in $\mathrm{Cl}(K_{\mathfrak{f}}/F) \setminus \mathrm{Cl}(K_{\mathfrak{f}}/L)$ we can find a character χ of $\mathrm{Cl}(\mathfrak{f})$ satisfying the conditions (2.4) in Lemma 2.5. Since the Euler factor of χ is 1 by the condition $\mathfrak{p}_k \mid \mathfrak{f}_\chi$ for all k, the value $S_{\mathfrak{f}}(\overline{\chi},\ g_{\mathfrak{f}})$ does not vanish by Proposition 2.2 and Remark 2.3(ii). On the other hand,

$$\begin{aligned} S_{\mathfrak{f}}(\overline{\chi},\ g_{\mathfrak{f}}) &= \sum_{\substack{C_1\in\mathrm{Cl}(\mathfrak{f})\\ C_1 \bmod \mathrm{Cl}(K_{\mathfrak{f}}/F)}} \sum_{\substack{C_2\in\mathrm{Cl}(K_{\mathfrak{f}}/F)\\ C_2 \bmod \mathrm{Cl}(K_{\mathfrak{f}}/L)}} \sum_{C_3\in\mathrm{Cl}(K_{\mathfrak{f}}/L)} \overline{\chi}(C_1C_2C_3)\log\big|g_{\mathfrak{f}}(C_1C_2C_3)\big| \\ &= \sum_{C_1}\overline{\chi}(C_1)\sum_{C_2}\overline{\chi}(C_2)\sum_{C_3}\log\big|g_{\mathfrak{f}}(C_0)^{\sigma(C_1)\sigma(C_2)\sigma(C_3)}\big| \quad \text{by } \chi|_{\mathrm{Cl}(K_{\mathfrak{f}}/L)} = 1 \text{ and (2.2)} \\ &= \sum_{C_1}\overline{\chi}(C_1)\sum_{C_2}\overline{\chi}(C_2)\log\big|\varepsilon^{\sigma(C_1)\sigma(C_2)}\big| \\ &= \sum_{C_1}\overline{\chi}(C_1)\Big(\sum_{C_2}\overline{\chi}(C_2)\Big)\log\big|\varepsilon^{\sigma(C_1)}\big| \quad \text{by the fact } \varepsilon\in F \\ &= 0 \quad \text{because } \chi(D)\neq 1 \text{ implies } \chi|_{\mathrm{Cl}(K_{\mathfrak{f}}/F)}\neq 1, \end{aligned}$$

which gives a contradiction. Therefore $L = F$ as desired. □

Remark 2.8. Observe that any nonzero power of ε generates L over K, too.

3. Action of Galois groups

In this section we shall determine Galois groups of ray class fields over ring class fields by adopting the idea of Gee and Stevenhagen([6], [16]).

For an integer $N(\geq 1)$, let $\zeta_N = e^{\frac{2\pi i}{N}}$ and $\Gamma(N) = \big\{\gamma\in\mathrm{SL}_2(\mathbb{Z}) : \gamma \equiv \left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right) \pmod N\big\}$. Further we let $\mathcal{F}_N$ be the field of modular functions whose Fourier coefficients belong to $\mathbb{Q}(\zeta_N)$.

Proposition 3.1. *$\mathcal{F}_N$ is a Galois extension of $\mathcal{F}_1 = \mathbb{Q}\big(j(\tau)\big)$ whose Galois group is isomorphic to $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)\} = G_N\cdot\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)\}$ where*

$$G_N = \left\{\begin{pmatrix}1&0\\0&d\end{pmatrix} \ :\ d\in(\mathbb{Z}/N\mathbb{Z})^*\right\}.$$

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

$$\sum_{n=-\infty}^{\infty} c_n q_\tau^{\frac{n}{N}} \mapsto \sum_{n=-\infty}^{\infty} c_n^{\sigma_d} q_\tau^{\frac{n}{N}}$$

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

$$h\mapsto h\circ\gamma'$$

as linear fractional transformation.

Proof. See [12] Chapter 6 Theorem 3. ☐

We need some transformation formulas of Siegel functions to apply the above proposition.

Proposition 3.2. *Let* $(r_1,\ r_2) \in \frac{1}{N}\mathbb{Z}^2 \setminus \mathbb{Z}^2$ *for* $N \geq 2$. *Then*

(i) $g_{(r_1,\ r_2)}^{12N}(\tau)$ *satisfies*

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

where $\langle X\rangle$ *is the fractional part of* $X \in \mathbb{R}$ *such that* $0 \leq \langle X\rangle < 1$.

(ii) $g_{(r_1,\ r_2)}^{12N}(\tau)$ *belongs to* $\mathcal{F}_N$ *and* α *in* $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1_2\} \cong \mathrm{Gal}(\mathcal{F}_N/\mathcal{F}_1)$ *acts on the function by*

$$\left(g_{(r_1,\ r_2)}^{12N}(\tau)\right)^{\alpha} = g_{(r_1,\ r_2)\alpha}^{12N}(\tau).$$

(iii) $g_{(r_1,\ r_2)}(\tau)$ *is integral over* $\mathbb{Z}[j(\tau)]$.

Proof. See [8] Proposition 2.4, Theorem 2.5 and Section 3. ☐

Now, let K be an imaginary quadratic field with discriminant d_K and define

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

from which we get $\mathcal{O}_K = \mathbb{Z}[\theta]$. We see from the main theorem of complex multiplication that for every integer $N(\geq 1)$

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

([12] Chapter 10 Corollary to Theorem 2). And, due to Gee and Stevenhagen we have the following proposition for the Shimura's reciprocity law which relates the class field theory to the theory of modular functions.

Proposition 3.3. *Let* $\min(\theta,\ \mathbb{Q}) = X^2 + B_\theta X + C_\theta \in \mathbb{Z}[X]$. *For every integer* $N(\geq 1)$ *the matrix group*

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

gives rise to the surjection

$$\begin{array}{ccc} W_{N,\ \theta} & \longrightarrow & \mathrm{Gal}(K_{(N)}/H) \\ \alpha & \mapsto & \Big(h(\theta) \mapsto h^{\alpha}(\theta)\Big) \end{array} \tag{3.2}$$

where $h \in \mathcal{F}_N$ *is defined and finite at* θ. *Its kernel is given by*

$$\begin{cases} \left\{\pm\begin{pmatrix}1&0\\0&1\end{pmatrix},\ \pm\begin{pmatrix}0&-1\\1&0\end{pmatrix}\right\} & \text{if } K = \mathbb{Q}(\sqrt{-1}) \\ \left\{\pm\begin{pmatrix}1&0\\0&1\end{pmatrix},\ \pm\begin{pmatrix}-1&-1\\1&0\end{pmatrix},\ \pm\begin{pmatrix}0&-1\\1&1\end{pmatrix}\right\} & \text{if } K = \mathbb{Q}(\sqrt{-3}) \\ \left\{\pm\begin{pmatrix}1&0\\0&1\end{pmatrix}\right\} & \text{otherwise.} \end{cases} \tag{3.3}$$

Proof. See [6] or [16]. ☐

The *ring class field* $H_\mathcal{O}$ *of the order* $\mathcal{O}$ *of conductor* $N(\geq 1)$ *in* K is by definition a finite abelian extension of K whose Galois group is isomorphic to $I_K(N\mathcal{O}_K)/P_{K,\,\mathbb{Z}}(N\mathcal{O}_K)$ via the Artin map where $P_{K,\,\mathbb{Z}}(N\mathcal{O}_K)$ is the subgroup of $P_K(N\mathcal{O}_K)$ generated by principal ideals $\alpha\mathcal{O}_K$ such that $\alpha \equiv a \pmod{N\mathcal{O}_K}$ for some integer a with $\gcd(a,\ N)=1$. Then, as is well-known $H_\mathcal{O}$ is contained in $K_{(N)}$.

Lemma 3.4. *Let* K *be an imaginary quadratic field with discriminant* d_K. *Then we have the following degree formulas:*

(i) *If* $\mathcal{O}$ *is the order of conductor* $N(\geq 1)$ *in* K, *then*

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

where h_K *is the class number of* K *and*

$$\left(\frac{d_K}{p}\right)=\begin{cases}\text{the Kronecker symbol} & \text{if } p=2\\ \text{the Legendre symbol} & \text{if } p \text{ is an odd prime.}\end{cases}$$

(ii) *If* $\mathfrak{f}\in I_K$, *then*

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

where φ *is the Euler function for ideals, namely*

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

for a power of prime ideal $\mathfrak{p}$ *(and we set* $\varphi(\mathcal{O}_K)=1$*).*

Proof. See [12] Chapter 8 Theorem 7 and [11] Chapter VI Theorem 1. One can also derive the statement (ii) directly from the exact sequence (2.1). □

Lemma 3.5. $\left(\begin{smallmatrix} t & 0\\ 0 & t\end{smallmatrix}\right)\in W_{N,\theta}$ *fixes* $j(N\theta)$.

Proof. Decompose $\left(\begin{smallmatrix} t & 0\\ 0 & t\end{smallmatrix}\right)\in W_{N,\theta}$ into $\left(\begin{smallmatrix} t & 0\\ 0 & t\end{smallmatrix}\right)=\left(\begin{smallmatrix} 1 & 0\\ 0 & t^2\end{smallmatrix}\right)\cdot\alpha\in G_N\cdot \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm\left(\begin{smallmatrix} 1 & 0\\ 0 & 1\end{smallmatrix}\right)\}$ as in Proposition 3.1 and let α' be a preimage of α 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 α' belongs to $\Gamma_0(N)=\{\gamma\in\mathrm{SL}_2(\mathbb{Z}):\gamma\equiv\left(\begin{smallmatrix} * & *\\ 0 & *\end{smallmatrix}\right)\pmod N\}$. We then obtain from Propositions 3.3 and 3.1 that

$$\begin{aligned}
\Big(j(N\theta)\Big)^{\left(\begin{smallmatrix} t & 0\\ 0 & t\end{smallmatrix}\right)} &= \Big(j(N\tau)\Big)^{\left(\begin{smallmatrix} t & 0\\ 0 & t\end{smallmatrix}\right)}(\theta)=\Big(j(N\tau)\Big)^{\left(\begin{smallmatrix} 1 & 0\\ 0 & t^2\end{smallmatrix}\right)\alpha}(\theta)\\
&= \Big(j(N\tau)\Big)^{\alpha}(\theta)\quad\text{because } j(N\tau) \text{ has rational Fourier coefficients([12] Chapter 4 Section 1)}\\
&= j(N\tau)\circ\alpha'(\theta)\\
&= j(N\theta)\quad \text{by the fact } \alpha'\in\Gamma_0(N) \text{ and } j(N\tau) \text{ is modular for } \Gamma_0(N)\text{([12] Chapter 6 Theorem 7).}
\end{aligned}$$

Therefore, this proves the lemma. □

Proposition 3.6. *Let* $\mathcal{O}$ *be the order of conductor* $N(\geq 1)$ *in* K. *Then the map in (3.2) induces an isomorphism*

$$\left\{\begin{pmatrix} t & 0\\ 0 & t\end{pmatrix}\ :\ t\in(\mathbb{Z}/N\mathbb{Z})^*\right\}\Big/\left\{\pm\begin{pmatrix} 1 & 0\\ 0 & 1\end{pmatrix}\right\}\stackrel{\sim}{\longrightarrow}\mathrm{Gal}(K_{(N)}/H_\mathcal{O}).$$

Proof. First, observe that the above map is well-defined and injective by Lemmas 3.5 and (3.3). Let

$$N=\prod_{a=1}^{A}p_a^{u_a}\prod_{b=1}^{B}q_b^{v_b}\prod_{c=1}^{C}r_c^{w_c}$$

be the prime factorization of N where each p_a (respectively, q_b and r_c) splits completely (respectively, is inert and ramified) in $K/\mathbb{Q}$ and $A,\ B,\ C\geq 0$. (We understand $\prod_1^0$ as 1.) Then we have

$$\left(\frac{d_K}{p_a}\right)=1,\quad \left(\frac{d_K}{q_b}\right)=-1,\quad \left(\frac{d_K}{r_c}\right)=0 \tag{3.4}$$

and the prime ideal factorization

$$N\mathcal{O}_K=\prod_{a=1}^{A}(\mathfrak{p}_a\overline{\mathfrak{p}}_a)^{u_a}\prod_{b=1}^{B}\mathfrak{q}_b^{v_b}\prod_{c=1}^{C}\mathfrak{r}_c^{2w_c}$$

with

$$\mathbf{N}_{K/\mathbb{Q}}(\mathfrak{p}_a)=\mathbf{N}_{K/\mathbb{Q}}(\overline{\mathfrak{p}}_a)=p_a,\quad \mathbf{N}_{K/\mathbb{Q}}(\mathfrak{q}_b)=q_b^2,\quad \mathbf{N}_{K/\mathbb{Q}}(\mathfrak{r}_c)=r_c. \tag{3.5}$$

And, we derive by Lemma 3.4 that

$$\begin{aligned}
&\#\ \mathrm{Gal}(K_{(N)}/H_\mathcal{O})=[K_{(N)}:H_\mathcal{O}]=\frac{[K_{(N)}:K]}{[H_\mathcal{O}:K]}\\
=\ &\frac{\varphi(N\mathcal{O}_K)w(N\mathcal{O}_K)}{2N\prod_{p|N}\left(1-\left(\frac{d_K}{p}\right)\frac{1}{p}\right)}\quad\text{by the facts } w_K=\#\ \mathcal{O}_K^*\text{ and }\mathcal{O}^*=\{\pm1\}\\
=\ &\frac{w(N\mathcal{O}_K)}{2}\frac{\prod_{a=1}^{A}\left((p_a-1)p_a^{u_a-1}\right)^2\prod_{b=1}^{B}(q_b^2-1)q_b^{2(v_b-1)}\prod_{c=1}^{C}(r_c-1)r_c^{2w_c-1}}{\prod_{a=1}^{A}p_a^{u_a-1}(p_a-1)\prod_{b=1}^{B}q_b^{v_b-1}(q_b+1)\prod_{c=1}^{C}r_c^{w_c}}\quad\text{by (3.4) and (3.5)}\\
=\ &\frac{w(N\mathcal{O}_K)}{2}\prod_{a=1}^{A}(p_a-1)p^{u_a-1}\prod_{b=1}^{B}(q_b-1)q_b^{v_b-1}\prod_{c=1}^{C}(r_c-1)r_c^{w_c-1}=\frac{w(N\mathcal{O}_K)}{2}\phi(N)\\
=\ &\#\ \left\{\left(\begin{smallmatrix}t&0\\0&t\end{smallmatrix}\right)\ :\ t\in(\mathbb{Z}/N\mathbb{Z})^*\right\}/\left\{\pm\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)\right\}
\end{aligned}$$

where ϕ is the Euler function for integers. This concludes the proposition. □

4. Ring class invariants

We shall make use of Theorem 2.7 to construct primitive generators of ring class fields as singular values of quotients of the Δ-function.

The following lemma was studied in [9], but we provide its proof for completeness.

Lemma 4.1. *Let $N\geq 1$. Then we have the relation*

$$\prod_{t=1}^{N-1}g_{(0,\ \frac{t}{N})}^{12}(\tau)=N^{12}\frac{\Delta(N\tau)}{\Delta(\tau)}$$

where the left hand side is regarded as 1 when $N=1$.

Proof. Note the identity

$$\frac{1-X^N}{1-X}=1+X+\cdots+X^{N-1}=\prod_{t=1}^{N-1}(1-\zeta_N^tX). \tag{4.1}$$

We then deduce that for $N \geq 2$

$$\begin{aligned}
\prod_{t=1}^{N-1} g_{(0,\ \frac{t}{N})}^{12}(\tau) &= \prod_{t=1}^{N-1}\Big(-q_\tau^{\frac{1}{12}}\zeta_{2N}^{-t}(1-\zeta_N^t)\prod_{n=1}^{\infty}(1-q_\tau^n\zeta_N^t)(1-q_\tau^n\zeta_N^{-t})\Big)^{12} \quad \text{by definition (1.2)}\\
&= q_\tau^{N-1}N^{12}\prod_{n=1}^{\infty}\left(\frac{1-q_\tau^{Nn}}{1-q_\tau^n}\right)^{24} \quad \text{by the identity (4.1)}\\
&= N^{12}\frac{\Delta(N\tau)}{\Delta(\tau)} \quad \text{by definition (1.1).}
\end{aligned}$$

□

Now we are ready to prove our main theorem.

Theorem 4.2. *Let K be an imaginary quadratic field with θ as in (3.1) and $\mathcal{O}$ be the order of conductor $N(\geq 2)$ in K. For the prime factorization*

$$N = \prod_{k=1}^{n} p_k^{e_k},$$

we set

$$N_S = \begin{cases} \prod_{k\in S} p_k & \text{if } S \text{ is a nomepty subset of } \{1,2,\cdots,n\}\\ 1 & \text{if } S=\emptyset. \end{cases}$$

If $\mathfrak{f} = N\mathcal{O}_K$ satisfies the assumption (2.3) in Lemma 2.5, then the singular value

$$\begin{cases} p_1^{12}\dfrac{\Delta(p_1^{e_1}\theta)}{\Delta(p_1^{e_1-1}\theta)} & \text{if } n=1\\ \displaystyle\prod_{S\subseteq\{1,2,\cdots,n\}}\Delta\Big(\frac{N}{N_S}\theta\Big)^{(-1)^{\#S}} & \text{if } n\geq 2 \end{cases} \tag{4.2}$$

generates $H_{\mathcal{O}}$ over K as a real algebraic integer.

Proof. If $\mathfrak{f} = N\mathcal{O}_K$, then $g_{\mathfrak{f}}(C_0) = g_{(0,\ \frac{1}{N})}^{12N}(\theta)$ by definition. And, we get that

$$\begin{aligned}
&\begin{cases} \mathbf{N}_{K_{\mathfrak{f}}/H_{\mathcal{O}}}\Big(g_{\mathfrak{f}}(C_0)\Big) & \text{if } N=2\\ \mathbf{N}_{K_{\mathfrak{f}}/H_{\mathcal{O}}}\Big(g_{\mathfrak{f}}(C_0)\Big)^2 & \text{if } N\geq 3 \end{cases}\\
&= \prod_{\substack{1\leq t\leq N-1\\ \gcd(t,\ N)=1}}\Big(g_{(0,\ \frac{1}{N})}^{12N}(\theta)\Big)^{\left(\begin{smallmatrix} t & 0\\ 0 & t\end{smallmatrix}\right)} \quad \text{by Proposition 3.6}\\
&= \prod_{\substack{1\leq t\leq N-1\\ \gcd(t,\ N)=1}}\Big(g_{(0,\ \frac{1}{N})}^{12N}\Big)^{\left(\begin{smallmatrix} t & 0\\ 0 & t\end{smallmatrix}\right)}(\theta) \quad \text{by Proposition 3.3}\\
&= \prod_{\substack{1\leq t\leq N-1\\ \gcd(t,\ N)=1}} g_{(0,\ \frac{t}{N})}^{12N}(\theta) \quad \text{by Proposition 3.2(ii)}
\end{aligned}$$

$$= \prod_{S\subseteq\{1,2,\cdots,n\}} \Big(\prod_{\substack{1\leq t\leq N-1\\ N_S|\ t}} g^{12}_{(0,\ \frac{t}{N})}(\theta)\Big)^{N(-1)^{\#S}} \quad \text{by inclusion-exclusion principle}$$

$$= \prod_{S\subseteq\{1,2,\cdots,n\}} \Big(\prod_{w=1}^{\frac{N}{N_S}-1} g^{12}_{(0,\ \frac{N_S w}{N})}(\theta)\Big)^{N(-1)^{\#S}}$$

$$= \prod_{S\subseteq\{1,2,\cdots,n\}} \Big(\Big(\frac{N}{N_S}\Big)^{12}\frac{\Delta(\frac{N}{N_S}\theta)}{\Delta(\theta)}\Big)^{N(-1)^{\#S}} \quad \text{by Lemma 4.1} \tag{4.3}$$

which is a generator of $H_\mathcal{O}$ over K by Theorem 2.7 and Remark 2.8. On the other hand, the value $\mathbf{N}_{K_\mathfrak{f}/H_\mathcal{O}}\big(g_\mathfrak{f}(C_0)\big)$ is an algebraic integer by Proposition 3.2(iii) and the fact that $j(\theta)$ is an algebraic integer([12] or [15]). Furthermore, each factor $\frac{\Delta(\frac{N}{N_S}\theta)}{\Delta(\theta)}$ appeared in (4.3) belongs to the ring class field of the order of conductor $\frac{N}{N_S}$ in K as a real algebraic number([12] Chapter 12 Corollary to Theorem 1). Therefore the value in (4.3) without N-th power generates $H_\mathcal{O}$ over K as an algebraic integer. Here, we further observe that

$$\prod_{S\subseteq\{1,2,\cdots,n\}} \Big(\Big(\frac{N}{N_S}\Big)^{12}\frac{\Delta(\frac{N}{N_S}\theta)}{\Delta(\theta)}\Big)^{(-1)^{\#S}}$$

$$= \Big(\frac{N^{12}}{\Delta(\theta)}\Big)^{\sum_{S\subseteq\{1,2,\cdots,n\}}(-1)^{\#S}} \prod_{S\subseteq\{1,2,\cdots,n\}} N_S^{-12(-1)^{\#S}} \prod_{S\subseteq\{1,2,\cdots,n\}} \Delta\Big(\frac{N}{N_S}\theta\Big)^{(-1)^{\#S}}$$

$$= \begin{cases} \Big(\frac{p_1^{12e_1}}{\Delta(\theta)}\Big)^{1-1} p_1^{12}\Delta(p_1^{e_1}\theta)\Delta(p_1^{e_1-1}\theta)^{-1} & \text{if } n=1\\ \Big(\frac{N^{12}}{\Delta(\theta)}\Big)^{\sum_{k=0}^{n}\binom{n}{k}(-1)^k} \prod_{k=1}^{n} p_k^{-12\sum_{\ell=1}^{n}\binom{n-1}{\ell-1}(-1)^\ell} \prod_{S\subseteq\{1,2,\cdots,n\}} \Delta\Big(\frac{N}{N_S}\theta\Big)^{(-1)^{\#S}} & \text{if } n\geq 2 \end{cases}$$

$$= \begin{cases} p_1^{12}\frac{\Delta(p_1^{e_1}\theta)}{\Delta(p_1^{e_1-1}\theta)} & \text{if } n=1\\ \prod_{S\subseteq\{1,2,\cdots,n\}} \Delta\Big(\frac{N}{N_S}\theta\Big)^{(-1)^{\#S}} & \text{if } n\geq 2. \end{cases}$$

This completes the proof. □

Remark 4.3. For a given imaginary quadratic field K, let $\mathcal{O}$ be the order of conductor $N(\geq 2)$ in K with

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

We denote by r_k the ramification index of p_k in $K/\mathbb{Q}$ for each $k=1,\cdots,n$. Assume first that

$$\text{each } p_k \text{ is an odd prime which is inert or ramified in } K/\mathbb{Q}. \tag{4.4}$$

Then we have the factorization

$$N\mathcal{O}_K = \prod_{k=1}^{n} \mathfrak{p}_k^{r_k e_k} \quad \text{with} \quad \mathbf{N}_{K/\mathbb{Q}}(\mathfrak{p}_k) = p_k^{\frac{2}{r_k}},$$

and

$$\widehat{\varepsilon}_k=\left\{\begin{array}{ll}\frac{1}{w_K}(p_1^{\frac{2}{r_1}}-1)p_1^{2e_1-\frac{2}{r_1}} & \text{if } n=1\\ (p_k^{\frac{2}{r_k}}-1)p_k^{2e_k-\frac{2}{r_k}} & \text{if } n\geq 2\end{array}\right.,\quad \varepsilon_k=\frac{\prod_{\ell=1}^n(p_\ell^{\frac{2}{r_\ell}}-1)p_\ell^{2e_\ell-\frac{2}{r_\ell}}}{(p_k^{\frac{2}{r_k}}-1)p_k^{2e_k-\frac{2}{r_k}}}\quad (k=1,\cdots,n)$$

by Remark 2.6 and

$$\#\ \mathrm{Cl}(K_{(N)}/H_\mathcal{O})=\frac{1}{2}\prod_{k=1}^n(p_k-1)p_k^{e_k-1}$$

by Proposition 3.6. Assume further that

$$e_k+1>\frac{2}{r_k}\quad\text{for all } k=1,\cdots,n\quad\text{and}\quad\left\{\begin{array}{ll}\gcd(p_1,\ w_K)=1 & \text{if } n=1\\ \gcd\left(\prod_{k=1}^n p_k,\ \prod_{k=1}^n(p_k^{\frac{2}{r_k}}-1)\right)=1 & \text{if } n\geq 2.\end{array}\right. \tag{4.5}$$

Then, since

$$p_k\nmid\varepsilon_k\quad\text{and}\quad \mathrm{ord}_{p_k}(\widehat{\varepsilon}_k)=2e_k-\frac{2}{r_k}\ >\ \mathrm{ord}_{p_k}\big(\#\ \mathrm{Cl}(K_{(N)}/H_\mathcal{O})\big)=e_k-1\quad(k=1,\cdots,n),$$

we can take $\nu_k=p_k$ as for the assumption (2.3) in Lemma 2.5. Therefore one can apply Theorem 4.2 under the assumptions (4.4) and (4.5).

Example 4.4. If $K=\mathbb{Q}(\sqrt{-7})$ and $N=7$, then $h_K=1$([4]), in other words, $K=H$. Let $\mathcal{O}$ be the order of conductor N in K. Then we get by Propositions 3.3 and 3.6 that

$$\begin{aligned}\mathrm{Gal}(H_\mathcal{O}/K)\ &\cong\ \Big(W_{7,\,\theta}/\big\{\pm\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)\big\}\Big)\Big/\Big(\big\{\left(\begin{smallmatrix}t&0\\0&t\end{smallmatrix}\right)\ :\ t\in(\mathbb{Z}/7\mathbb{Z})^*\big\}/\big\{\pm\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)\big\}\Big)\\ &=\ \Big\{\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)\cdot\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right),\ \left(\begin{smallmatrix}1&0\\0&2\end{smallmatrix}\right)\cdot\left(\begin{smallmatrix}-1&-2\\4&7\end{smallmatrix}\right),\ \left(\begin{smallmatrix}1&0\\0&2\end{smallmatrix}\right)\cdot\left(\begin{smallmatrix}7&12\\-10&-17\end{smallmatrix}\right),\\ &\qquad\left(\begin{smallmatrix}1&0\\0&4\end{smallmatrix}\right)\cdot\left(\begin{smallmatrix}-13&-16\\9&11\end{smallmatrix}\right),\ \left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)\cdot\left(\begin{smallmatrix}-5&-16\\1&3\end{smallmatrix}\right),\ \left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)\cdot\left(\begin{smallmatrix}-3&-16\\1&5\end{smallmatrix}\right),\ \left(\begin{smallmatrix}1&0\\0&4\end{smallmatrix}\right)\cdot\left(\begin{smallmatrix}-16&-9\\9&5\end{smallmatrix}\right)\Big\}\end{aligned}$$

where $\theta=\frac{-1+\sqrt{-7}}{2}$. Note that we express here elements of $\mathrm{Gal}(H_\mathcal{O}/K)$ in the form of

$$\left(\begin{smallmatrix}1&0\\0&d\end{smallmatrix}\right)\ \text{for some } d\in(\mathbb{Z}/7\mathbb{Z})^*\cdot\text{an element of } \mathrm{SL}_2(\mathbb{Z}).$$

On the other hand, since 7 is ramified in $K/\mathbb{Q}$ and $w_K=2$, the assumptions (4.4) and (4.5) in Remark 4.3 (or, the assumption (5.22) in Remark 5.5) are satisfied. Hence the singular value $7^{12}\frac{\Delta(7\theta)}{\Delta(\theta)}$ generates $H_\mathcal{O}$ over K by Theorem 4.2 (or, Theorem 5.4). Furthermore, since the function $\frac{\Delta(7\tau)}{\Delta(\tau)}$ has rational Fourier coefficients and belongs to $\mathcal{F}_7$([12] Chapter 11 Theorem 4), we obtain its minimal polynomial by Propositions 3.3 and 3.1 as

$$\begin{aligned}
\min\Big(7^{12}\tfrac{\Delta(7\theta)}{\Delta(\theta)},\ K\Big) &= \Big(X-7^{12}\tfrac{\Delta(7\tau)}{\Delta(\tau)}\circ\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)(\theta)\Big)\Big(X-7^{12}\tfrac{\Delta(7\tau)}{\Delta(\tau)}\circ\left(\begin{smallmatrix}-1&-2\\4&7\end{smallmatrix}\right)(\theta)\Big)\\
&\quad\Big(X-7^{12}\tfrac{\Delta(7\tau)}{\Delta(\tau)}\circ\left(\begin{smallmatrix}7&12\\-10&-17\end{smallmatrix}\right)(\theta)\Big)\Big(X-7^{12}\tfrac{\Delta(7\tau)}{\Delta(\tau)}\circ\left(\begin{smallmatrix}-13&-16\\9&11\end{smallmatrix}\right)(\theta)\Big)\\
&\quad\Big(X-7^{12}\tfrac{\Delta(7\tau)}{\Delta(\tau)}\circ\left(\begin{smallmatrix}-5&-16\\1&3\end{smallmatrix}\right)(\theta)\Big)\Big(X-7^{12}\tfrac{\Delta(7\tau)}{\Delta(\tau)}\circ\left(\begin{smallmatrix}-3&-16\\1&5\end{smallmatrix}\right)(\theta)\Big)\\
&\quad\Big(X-7^{12}\tfrac{\Delta(7\tau)}{\Delta(\tau)}\circ\left(\begin{smallmatrix}-16&-9\\9&5\end{smallmatrix}\right)(\theta)\Big)\\
&= X^7+234857X^6+24694815621X^5+295908620105035X^4\\
&\quad+943957383096939785X^3+356807315211847521X^2\\
&\quad+38973886319454982X-117649.
\end{aligned}$$

On the other hand, if we compare its coefficients with those of the minimal polynomial of the classical invariant $j(7\theta)$, we see in a similar fashion that the latter are much bigger than the former as follows:

$$\begin{aligned}
\min\big(j(7\theta),\ K\big) &= X^7+18561099067532582351348250X^6+54379116263846797396254926859375X^5\\
&\quad+3445143985948385966658768373473428439956476464 84375X^4\\
&\quad+1009848457088842748174122781381460720529620832094970703125X^3\\
&\quad+1480797351289795967859364968037513969226011238564633514404296875X^2\\
&\quad-397265360164906648432657360525140674130401547352179687881469726 5625X\\
&\quad+479157656234174703454827666127009330510502726757310384511947631835 9375.
\end{aligned}$$

Example 4.5. Let $K=\mathbb{Q}(\sqrt{-5})$ and $\mathcal{O}$ be the order of conductor $N=6(=2\cdot 3)$ in K. Then one can readily check that $N\mathcal{O}_K$ satisfies neither the assumption (2.3) in Lemma 2.5 nor the assumption (5.22) in Remark 5.5. Even in this case, however, we will see that our method is still valid. Therefore, it is worth of studying how much further one can release from the assumption (2.3) in Lemma 2.5 (or, the assumption (5.22) in Remark 5.5).

Observe that $h_K=2([4])$ and $[H_\mathcal{O}:K]=8$ by Lemma 3.4(i). Since $h_K=2$, there are two reduced positive definite binary quadratic forms of discriminant $d_K=-20$

$$Q_1=X^2+5Y^2\quad\text{and}\quad Q_2=2X^2+2XY+3Y^2.$$

We associate to each $Q_k(k=1,\ 2)$ a matrix in $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ and a CM-point as follows:

$$\begin{cases}\beta_1=\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right), & \theta_1=\sqrt{-5} & \text{for } Q_1\\ \beta_2=\left(\begin{smallmatrix}1&5\\3&2\end{smallmatrix}\right), & \theta_2=\frac{-1+\sqrt{-5}}{2} & \text{for } Q_2.\end{cases}$$

Then we see from Lemma 20 in [6] that

$$\mathrm{Gal}(H/K)=\Big\{\big(h(\theta)\mapsto h^{\beta_k}(\theta_k)\big)\big|_H\ :\ k=1,\ 2\Big\}$$

where $h\in\mathcal{F}_N$ is defined and finite at $\theta=\sqrt{-5}$. Furthermore, it follows from Propositions 3.3 and 3.6 that

$$\mathrm{Gal}(H_\mathcal{O}/H)\cong\Big\{\alpha_1=\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right),\ \alpha_2=\left(\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right),\ \alpha_3=\left(\begin{smallmatrix}2&3\\3&2\end{smallmatrix}\right),\ \alpha_4=\left(\begin{smallmatrix}3&2\\2&3\end{smallmatrix}\right)\Big\}.$$

Hence we achieve that

$$\mathrm{Gal}(H_{\mathcal{O}}/K)=\left\{\big(h(\theta)\mapsto h^{\alpha_\ell\beta_k}(\theta_k)\big)|_{H_{\mathcal{O}}}\ :\ \ell=1,\cdots,4,\ k=1,\ 2\right\}$$

where $h\in\mathcal{F}_N$ is defined and finite at θ. On the other hand, the conjugates of the singular value $\frac{\Delta(6\theta)\Delta(\theta)}{\Delta(2\theta)\Delta(3\theta)}$ estimated according to Theorem 4.2 are

$$x_{\ell,\ k}=\left(\frac{\Delta(6\tau)\Delta(\tau)}{\Delta(2\tau)\Delta(3\tau)}\right)^{\alpha_\ell\beta_k}(\theta_k)\quad(\ell=1,\cdots,4,\ k=1,\ 2)$$

possibly with some multiplicity. And, since the function $\frac{\Delta(6\tau)\Delta(\tau)}{\Delta(2\tau)\Delta(3\tau)}\in\mathcal{F}_N$ has rational Fourier coefficients, the action of each $\alpha_\ell\beta_k$ on it can be performed as in the previous example. Thus the minimal polynomial of $\frac{\Delta(6\theta)\Delta(\theta)}{\Delta(2\theta)\Delta(3\theta)}$ becomes a divisor of

$$\begin{aligned}\textstyle\prod_{\ell=1,\cdots,4,\ k=1,\ 2}(X-x_{\ell,\ k}) \;=\;& X^8-1304008X^7+16670918428X^6+30056736254344X^5\\ &+23344024601638470X^4+7327603919934344X^3\\ &+1949665164230428X^2-1597207512008X+1.\end{aligned}$$

This polynomial is, however, irreducible and hence the singular value $\frac{\Delta(6\theta)\Delta(\theta)}{\Delta(2\theta)\Delta(3\theta)}$ should be a primitive generator of $H_{\mathcal{O}}$ over K.

5. Another approach

We shall develop a different lemma which substitutes for Lemma 2.5, from which we are able to find more N's in Theorem 4.2.

Throughout this section $K(\neq\mathbb{Q}(\sqrt{-1}),\ \mathbb{Q}(\sqrt{-3}))$ is also an imaginary quadratic field with θ as in (3.1). For an integer $N\geq 2$ let

$$\mathfrak{f}=N\mathcal{O}_K=\prod_{k=1}^{n}\mathfrak{p}_k^{e_k}$$

and $\mathcal{O}$ be the order of conductor N in K. We use the same notations $\pi_{\mathfrak{f}}$, ι, ι_k, v_k, $\widetilde{\Phi}_{\mathfrak{f}}$ as in Section 2. And, by $\mathrm{Cl}(H_{\mathcal{O}}/K)$ we mean the quotient group of $\mathrm{Cl}(\mathfrak{f})$ corresponding to $\mathrm{Gal}(H_{\mathcal{O}}/K)$ via the Artin map, that is,

$$\mathrm{Cl}(H_{\mathcal{O}}/K)=\mathrm{Cl}(\mathfrak{f})/\mathrm{Cl}(K_{\mathfrak{f}}/H_{\mathcal{O}}). \tag{5.1}$$

We further let $\mathrm{Cl}(H_{\mathcal{O}}/H)$ stand for the subgroup of $\mathrm{Cl}(H_{\mathcal{O}}/K)$ corresponding to $\mathrm{Gal}(H_{\mathcal{O}}/H)$.

Setting

$$\check{\Psi}_{\mathfrak{f}}=\big(\mathrm{Cl}(\mathfrak{f})\longrightarrow\mathrm{Cl}(H_{\mathcal{O}}/K)\big)\circ\widetilde{\Phi}_{\mathfrak{f}}\ :\ \pi_{\mathfrak{f}}(\mathcal{O}_K)^*\longrightarrow\mathrm{Cl}(H_{\mathcal{O}}/K), \tag{5.2}$$

we obtain by the exact sequence (2.1) and Galois theory another exact sequence

$$1\longrightarrow\pi_{\mathfrak{f}}(\mathcal{O}_K)^*/\mathrm{Ker}(\check{\Psi}_{\mathfrak{f}})\longrightarrow\mathrm{Cl}(H_{\mathcal{O}}/K)\longrightarrow\mathrm{Cl}(\mathcal{O}_K)\longrightarrow 1 \tag{5.3}$$

with

$$\check{\Psi}_{\mathfrak{f}}\big(\pi_{\mathfrak{f}}(\mathcal{O}_K)^*\big)=\mathrm{Cl}(H_{\mathcal{O}}/H). \tag{5.4}$$

And, we know by the fact $w_K=2$ and Lemma 3.4 that

$$\#\pi_{\mathfrak{f}}(\mathcal{O}_K)^*/\pi_{\mathfrak{f}}(\mathbb{Z})^*=\frac{\varphi(\mathfrak{f})}{\phi(N)}\quad\text{and}\quad[H_{\mathcal{O}}:H]=\frac{\varphi(\mathfrak{f})}{\phi(N)}.$$

On the other hand, since $\mathrm{Cl}(K_{\mathfrak{f}}/H_{\mathcal{O}})=P_{K,\ \mathbb{Z}}(\mathfrak{f})/P_{K,\ 1}(\mathfrak{f})$ by definition of $H_{\mathcal{O}}$, we get $\pi_{\mathfrak{f}}(\mathbb{Z})^*\subseteq\mathrm{Ker}(\check{\Psi}_{\mathfrak{f}})$; hence we achieve

$$\mathrm{Ker}(\check{\Psi}_{\mathfrak{f}})=\pi_{\mathfrak{f}}(\mathbb{Z})^*. \tag{5.5}$$

Lemma 5.1. *Let G be a finite abelian group and H be a subgroup of G. Then there is a canonical isomorphism between character groups*

$$\begin{array}{rcl}\big\{\textit{characters of } G \textit{ which are trivial on } H\big\} & \longrightarrow & \big\{\textit{characters of } G/H\big\} \\ \chi & \mapsto & \big(gH \mapsto \chi(g)\ :\ g\in G\big).\end{array} \tag{5.6}$$

Proof. One can readily check that the map in (5.6) is a well-defined injection. For surjectivity, let ψ be a character of G/H. Then the character

$$\chi = \psi\circ(G\longrightarrow G/H)$$

of G maps to ψ via the map in (5.6), which claims the surjectivity. □

Thus we have a canonical isomorphism

$$\big\{\text{characters of } \mathrm{Cl}(\mathfrak{f}) \text{ which are trivial on } \mathrm{Cl}(K_\mathfrak{f}/H_\mathcal{O})\big\} \longrightarrow \big\{\text{characters of } \mathrm{Cl}(H_\mathcal{O}/K)\big\} \tag{5.7}$$

by Lemma 5.1 and definition (5.1). For any character ψ of $\mathrm{Cl}(H_\mathcal{O}/K)$ we define

$$\check{\psi} = \psi\circ\check{\Psi}_\mathfrak{f} \quad\text{and}\quad \check{\psi}_k = \check{\psi}\circ\iota\circ\iota_k \quad (k=1,\cdots,n).$$

If χ maps to ψ via the map in (5.7), then we derive

$$\begin{array}{rcl}\widetilde{\chi} & = & \chi\circ\widetilde{\Phi}_\mathfrak{f} = \psi\circ\big(\mathrm{Cl}(\mathfrak{f})\longrightarrow \mathrm{Cl}(H_\mathcal{O}/K)\big)\circ\widetilde{\Phi}_\mathfrak{f} \quad \text{by the proof of Lemma 5.1} \\ & = & \psi\circ\check{\Psi}_\mathfrak{f} = \check{\psi} \quad \text{by definition (5.2)}\end{array}$$

so that

$$\widetilde{\chi}_k = \check{\psi}_k \quad \text{for all } k=1,\cdots,n.$$

Lemma 5.2. *Let*

$$\begin{array}{rcl} U & = & \big\{\textit{characters of } \mathrm{Cl}(H_\mathcal{O}/K) \textit{ which are trivial on } \mathrm{Cl}(H_\mathcal{O}/H)\big\} \\ V & = & \big\{\textit{characters of } \mathrm{Cl}(H_\mathcal{O}/H)\big\} \\ W & = & \big\{\textit{characters of } \mathrm{Cl}(H_\mathcal{O}/K)\big\} \\ G_k & = & \widehat{v}_k\circ\iota^{-1}\big(\pi_\mathfrak{f}(\mathbb{Z})^*\big) \quad (k=1,\cdots,n)\end{array}$$

where

$$\widehat{v}_k\ :\ \prod_{\ell=1}^{n}\pi_{\mathfrak{p}_\ell^{e_\ell}}(\mathcal{O}_K)^* \longrightarrow \pi_{\mathfrak{p}_1^{e_1}}(\mathcal{O}_K)^*\times\cdots\times\pi_{\mathfrak{p}_{k-1}^{e_{k-1}}}(\mathcal{O}_K)^*\times\pi_{\mathfrak{p}_{k+1}^{e_{k+1}}}(\mathcal{O}_K)^*\times\cdots\times\pi_{\mathfrak{p}_n^{e_n}}(\mathcal{O}_K)^*$$

is the natural projection which deletes the k-th component. For each character $\psi\in V$, fix a character $\psi'\in W$ which extends ψ (by Lemma 2.4).

(i) *There is a bijective map*

$$\begin{array}{rcl} U\times V & \longrightarrow & W \\ (\chi,\ \psi) & \mapsto & \chi\cdot\psi'.\end{array}$$

(ii) *We have the inequality*

$$\#\big\{\xi\in W\ :\ \check{\xi}_k = 1\big\} \le h_K\frac{\#\pi_\mathfrak{f}(\mathcal{O}_K)^*}{\#\pi_{\mathfrak{p}_k^{e_k}}(\mathcal{O}_K)^*\cdot\#G_k} \quad (k=1,\cdots,n).$$

Proof. (i) We see from Lemma 5.1 that both $U \times V$ and W have the same size. Hence it suffices to show that the above map is injective, which is straightforward.
(ii) Without loss of generality it suffices to show that there is an injective map

$$S = \{\xi \in W \ : \ \check{\xi}_n = 1\} \longrightarrow U \times \left\{\text{characters of } \prod_{k=1}^{n-1} \pi_{\mathfrak{p}_k^{e_k}}(\mathcal{O}_K)^* \Big/ G_n\right\},$$

because $\#U = h_K$ by Lemma 5.1 and $\# \prod_{k=1}^{n-1} \pi_{\mathfrak{p}_k^{e_k}}(\mathcal{O}_K)^*/G_n = \frac{\#\pi_\mathfrak{f}(\mathcal{O}_K)^*}{\#\pi_{\mathfrak{p}_n^{e_n}}(\mathcal{O}_K)^* \cdot \#G_n}$.

Let $\xi \in S$. Then as an element of W, ξ is of the form $\chi \cdot \psi'$ for some $\chi \in U$ and $\psi \in V$ by (i). And, by (5.4) and the fact $\chi \in U$ we get

$$\check{\chi} = \chi \circ \check{\Psi}_\mathfrak{f} = 1,$$

from which it follows that

$$1 = \check{\xi}_n = (\check{\chi} \cdot \check{\psi}')_n = \check{\psi}'_n. \tag{5.8}$$

We further deduce by (5.4) that

$$\check{\psi}' = \psi'|_{\check{\Psi}_\mathfrak{f}\left(\pi_\mathfrak{f}(\mathcal{O}_K)^*\right)} \circ \check{\Psi}_\mathfrak{f} = \psi'|_{\mathrm{Cl}(H_\mathcal{O}/H)} \circ \check{\Psi}_\mathfrak{f} = \psi \circ \check{\Psi}_\mathfrak{f}. \tag{5.9}$$

On the other hand, if β is a character of $\prod_{k=1}^{n} \pi_{\mathfrak{p}_k^{e_k}}(\mathcal{O}_K)^*$ defined by

$$\beta = \psi \circ \check{\Psi}_\mathfrak{f} \circ \iota, \tag{5.10}$$

then we derive that

$$\begin{aligned} \beta \circ \iota_n\left(\pi_{\mathfrak{p}_n^{e_n}}(\mathcal{O}_K)^*\right) &= \psi \circ \check{\Psi}_\mathfrak{f} \circ \iota \circ \iota_n\left(\pi_{\mathfrak{p}_n^{e_n}}(\mathcal{O}_K)^*\right) \\ &= \check{\psi}' \circ \iota \circ \iota_n\left(\pi_{\mathfrak{p}_n^{e_n}}(\mathcal{O}_K)^*\right) \quad \text{by (5.9)} \\ &= \check{\psi}'_n\left(\pi_{\mathfrak{p}_n^{e_n}}(\mathcal{O}_K)^*\right) = 1 \quad \text{by (5.8)}, \end{aligned}$$

which implies

$$\iota_n\left(\pi_{\mathfrak{p}_n^{e_n}}(\mathcal{O}_K)^*\right) \subseteq \mathrm{Ker}(\beta). \tag{5.11}$$

Furthermore, we have

$$\beta \circ \iota^{-1}\left(\pi_\mathfrak{f}(\mathbb{Z})^*\right) = \psi \circ \check{\Psi}_\mathfrak{f}\left(\pi_\mathfrak{f}(\mathbb{Z})^*\right) = 1 \quad \text{by (5.5)},$$

which claims

$$\iota^{-1}\left(\pi_\mathfrak{f}(\mathbb{Z})^*\right) \subseteq \mathrm{Ker}(\beta). \tag{5.12}$$

Hence β can be written as

$$\beta = \gamma \circ \left(\prod_{k=1}^{n} \pi_{\mathfrak{p}_k^{e_k}}(\mathcal{O}_K)^* \longrightarrow \prod_{k=1}^{n} \pi_{\mathfrak{p}_k^{e_k}}(\mathcal{O}_K)^* \Big/ \left\langle \iota_n\left(\pi_{\mathfrak{p}_n^{e_n}}(\mathcal{O}_K)^*\right),\ \iota^{-1}\left(\pi_\mathfrak{f}(\mathbb{Z})^*\right)\right\rangle \right) \tag{5.13}$$

for a unique character γ of $\prod_{k=1}^{n} \pi_{\mathfrak{p}_k^{e_k}}(\mathcal{O}_K)^*/\left\langle \iota_n\left(\pi_{\mathfrak{p}_n^{e_n}}(\mathcal{O}_K)^*\right),\ \iota^{-1}\left(\pi_\mathfrak{f}(\mathbb{Z})^*\right)\right\rangle$ by Lemma 5.1, (5.11) and (5.12).

Now, we define a map

$$\begin{aligned} \kappa \ : \ S &\longrightarrow U \times \left\{\text{characters of } \prod_{k=1}^{n-1} \pi_{\mathfrak{p}_k^{e_k}}(\mathcal{O}_K)^* \Big/ G_n\right\} \\ \xi &\mapsto (\chi,\ \gamma \circ \widehat{\iota_n}) \end{aligned}$$

where

$$\widehat{\iota_n}\ :\ \prod_{k=1}^{n-1}\pi_{\mathfrak{p}_k^{e_k}}(\mathcal{O}_K)^*\Big/G_n\longrightarrow\prod_{k=1}^{n}\pi_{\mathfrak{p}_k^{e_k}}(\mathcal{O}_K)^*\Big/\big\langle\iota_n\big(\pi_{\mathfrak{p}_n^{e_n}}(\mathcal{O}_K)^*\big),\ \iota^{-1}\big(\pi_{\mathfrak{f}}(\mathbb{Z})^*\big)\big\rangle$$

is definitely a surjection by definition of G_n. To prove the injectivity of the map κ, assume that $\kappa(\xi_1)=\kappa(\xi_2)$ for some $\xi_1,\ \xi_2\in S$. Then, by (i) there are unique $\chi_1,\ \chi_2\in U$ and $\psi_1,\ \psi_2\in V$ such that $\xi_1=\chi_1\cdot\psi_1'$ and $\xi_2=\chi_2\cdot\psi_2'$. And, by definition of κ we get $\chi_1=\chi_2$. Let $\psi_\ell(\ell=1,\ 2)$ induce β_ℓ and γ_ℓ in the above paragraph (which explains β and γ constructed from ψ). Then, since $\widehat{\iota_n}$ is surjective, we obtain $\gamma_1=\gamma_2$ from the fact $\gamma_1\circ\widehat{\iota_n}=\gamma_2\circ\widehat{\iota_n}$, and so we have $\beta_1=\beta_2$ by (5.13). It then follows from the definition (5.10), the fact $\psi_1,\ \psi_2\in V$ and (5.4) that $\psi_1=\psi_2$, which concludes the injectivity of κ. This completes the proof. □

Lemma 5.3. *Let F be a field such that $K\subseteq F\subsetneq H_{\mathcal{O}}$. If*

$$2\#\pi_{\mathfrak{f}}(\mathbb{Z})^*\sum_{k=1}^{n}\frac{1}{\#\pi_{\mathfrak{p}_k^{e_k}}(\mathcal{O}_K)^*\cdot\#G_k}<1,\tag{5.14}$$

then there is a character χ of $\mathrm{Cl}(\mathfrak{f})$ *such that*

$$\chi|_{\mathrm{Cl}(K_{\mathfrak{f}}/H_{\mathcal{O}})}=1,\quad \chi|_{\mathrm{Cl}(K_{\mathfrak{f}}/F)}\neq 1\quad\textit{and}\quad \mathfrak{p}_k\mid\mathfrak{f}_\chi\quad\textit{for all } k=1,\cdots,n.\tag{5.15}$$

Proof. We first derive that

$$\begin{aligned}
&\#\big\{\text{characters }\chi\text{ of }\mathrm{Cl}(\mathfrak{f})\ :\ \chi|_{\mathrm{Cl}(K_{\mathfrak{f}}/H_{\mathcal{O}})}=1,\ \chi|_{\mathrm{Cl}(K_{\mathfrak{f}}/F)}\neq 1\big\}\\
=\ &\#\big\{\chi\text{ of }\mathrm{Cl}(\mathfrak{f})\ :\ \chi|_{\mathrm{Cl}(K_{\mathfrak{f}}/H_{\mathcal{O}})}=1\big\}-\#\big\{\chi\text{ of }\mathrm{Cl}(\mathfrak{f})\ :\ \chi|_{\mathrm{Cl}(K_{\mathfrak{f}}/F)}=1\big\}\\
=\ &\#\mathrm{Cl}(\mathfrak{f})/\mathrm{Cl}(K_{\mathfrak{f}}/H_{\mathcal{O}})-\#\mathrm{Cl}(\mathfrak{f})/\mathrm{Cl}(K_{\mathfrak{f}}/F)\quad\text{by Lemma 5.1}\\
=\ &[H_{\mathcal{O}}:K]-[F:K]=[H_{\mathcal{O}}:K]\left(1-\frac{1}{[H_{\mathcal{O}}:F]}\right)\geq\frac{1}{2}[H_{\mathcal{O}}:K]\quad\text{by the fact }F\subsetneq H_{\mathcal{O}}\\
=\ &\frac{h_K}{2}\#\pi_{\mathfrak{f}}(\mathcal{O}_K)^*/\pi_{\mathfrak{f}}(\mathbb{Z})^*\quad\text{from the exact sequence (5.3) and (5.5)}\\
>\ &h_K\#\pi_{\mathfrak{f}}(\mathcal{O}_K)^*\sum_{k=1}^{n}\frac{1}{\#\pi_{\mathfrak{p}_k^{e_k}}(\mathcal{O}_K)^*\cdot\#G_k}\quad\text{by the assumption (5.14).}
\end{aligned}$$

On the other hand, we get that

$$\begin{aligned}
&\#\big\{\chi\text{ of }\mathrm{Cl}(\mathfrak{f})\ :\ \chi|_{\mathrm{Cl}(K_{\mathfrak{f}}/H_{\mathcal{O}})}=1,\ \mathfrak{p}_k\nmid\mathfrak{f}_\chi\text{ for some }k\big\}\\
\leq\ &\#\big\{\chi\text{ of }\mathrm{Cl}(\mathfrak{f})\ :\ \chi|_{\mathrm{Cl}(K_{\mathfrak{f}}/H_{\mathcal{O}})}=1,\ \widetilde{\chi}_k=1\text{ for some }k\big\}\quad\text{by Lemma 2.1}\\
=\ &\#\big\{\xi\text{ of }\mathrm{Cl}(H_{\mathcal{O}}/K)\ :\ \check{\xi}_k=1\text{ for some }k\big\}\quad\text{by the argument followed by Lemma 5.1}\\
\leq\ &h_K\#\pi_{\mathfrak{f}}(\mathcal{O}_K)^*\sum_{k=1}^{n}\frac{1}{\#\pi_{\mathfrak{p}_k^{e_k}}(\mathcal{O}_K)^*\cdot\#G_k}\quad\text{by Lemma 5.2(ii).}
\end{aligned}$$

Therefore, there exists a character χ of $\mathrm{Cl}(\mathfrak{f})$ which satisfies the condition (5.15). □

Theorem 5.4. *If $\mathfrak{f}=N\mathcal{O}_K$ satisfies the assumption (5.14) in Lemma 5.3, then the singular value in (4.2) generates $H_{\mathcal{O}}$ over K as a real algebraic integer.*

Proof. Let $\varepsilon=\mathbf{N}_{K_{\mathfrak{f}}/H_O}\big(g_{\mathfrak{f}}(C_0)\big)$ and $F=K(\varepsilon)$ as a subfield of $H_{\mathcal{O}}$. Suppose that F is properly contained in $H_{\mathcal{O}}$, then there is a character χ of $\mathrm{Cl}(\mathfrak{f})$ satisfying the condition (5.15) in Lemma 5.3. Since $\mathfrak{p}_k\mid\mathfrak{f}_k$ for all $k=1,\cdots,n$, the Euler factor of χ in Proposition 2.2 is 1, and hence the value $S_{\mathfrak{f}}(\overline{\chi},\ g_{\mathfrak{f}})$ does not vanish by Remark 2.3(ii). On the other hand, we can derive $S_{\mathfrak{f}}(\overline{\chi},\ g_{\mathfrak{f}})=0$ by using the condition (5.15) of χ in exactly the same way as the proof of Theorem 2.7, which gives rise to a contradiction. Therefore $H_{\mathcal{O}} = K(\varepsilon)$, and hence we can apply the argument of Theorem 4.2 to complete the proof. □

Remark 5.5. Let

$$N = \prod_{a=1}^{A} s_a^{u_a} \prod_{b=1}^{B} q_b^{v_b} \prod_{c=1}^{C} r_c^{w_c}$$

be the prime factorization of N where each s_a (respectively, q_b and r_c) splits completely (respectively, is inert and ramified) in $K/\mathbb{Q}$ and $A,\ B,\ C \geq 0$. Then we have the prime ideal factorization

$$\mathfrak{f} = N\mathcal{O}_K = \prod_{a=1}^{A} (\mathfrak{s}_a\bar{\mathfrak{s}}_a)^{u_a} \prod_{b=1}^{B} \mathfrak{q}_b^{v_b} \prod_{c=1}^{C} \mathfrak{r}_c^{2w_c}$$

with

$$\mathbf{N}_{K/\mathbb{Q}}(\mathfrak{s}_a) = \mathbf{N}_{K/\mathbb{Q}}(\bar{\mathfrak{s}}_a) = s_a, \quad \mathbf{N}_{K/\mathbb{Q}}(\mathfrak{q}_b) = q_b^2, \quad \mathbf{N}_{K/\mathbb{Q}}(\mathfrak{r}_c) = r_c.$$

Now, for the sake of convenience, we let

$$\mathfrak{f} = \prod_{k=1}^{2A+B+C} \mathfrak{p}_k^{e_k}$$

with

$$(\mathfrak{p}_k,\ e_k) = \begin{cases} (\mathfrak{s}_k,\ u_k) & \text{for } k = 1, \cdots, A \\ (\bar{\mathfrak{s}}_{k-A},\ u_{k-A}) & \text{for } k = A+1, \cdots, 2A \\ (\mathfrak{q}_{k-2A},\ v_{k-2A}) & \text{for } k = 2A+1, \cdots, 2A+B \\ (\mathfrak{r}_{k-2A-B},\ 2w_{k-2A-B}) & \text{for } k = 2A+B+1, \cdots, 2A+B+C, \end{cases} \tag{5.16}$$

and consider the surjection

$$\mu_k = \widehat{v}_k \circ \iota^{-1} \ :\ \pi_{\mathfrak{f}}(\mathbb{Z})^* \longrightarrow G_k \ \big(\subseteq \pi_{\mathfrak{p}_1^{e_1}}(\mathcal{O}_K)^* \times \cdots \times \pi_{\mathfrak{p}_{k-1}^{e_{k-1}}}(\mathcal{O}_K)^* \times \pi_{\mathfrak{p}_{k+1}^{e_{k+1}}}(\mathcal{O}_K)^* \times \cdots \times \pi_{\mathfrak{p}_n^{e_n}}(\mathcal{O}_K)^*\big).$$

If $m \pmod{\mathfrak{f}} \in \pi_{\mathfrak{f}}(\mathbb{Z})^*$ belongs to $\mathrm{Ker}(\mu_k)$, then

$$\begin{aligned} (\underbrace{1,\ \cdots,\ 1}_{n-1}) &= \mu_k\big(m \pmod{\mathfrak{f}}\big) = \widehat{v}_k \circ \iota^{-1}\big(m \pmod{\mathfrak{f}}\big) \\ &= \big(m \pmod{\mathfrak{p}_1^{e_1}},\ \cdots,\ m \pmod{\mathfrak{p}_{k-1}^{e_{k-1}}},\ m \pmod{\mathfrak{p}_{k+1}^{e_{k+1}}},\ \cdots,\ m \pmod{\mathfrak{p}_n^{e_n}}\big), \end{aligned} \tag{5.17}$$

which shows

$$\iota^{-1}\big(\mathrm{Ker}(\mu_k)\big) \subseteq \iota_k\big(\pi_{\mathfrak{p}_k^{e_k}}(\mathbb{Z})^*\big) = \big\{(1,\ \cdots,\ 1,\ t \pmod{\mathfrak{p}_k^{e_k}},\ 1,\ \cdots,\ 1)\ :\ t \in \mathbb{Z} \text{ which is prime to } \mathfrak{p}_k\big\}.$$

Hence, this gives the inequality

$$\#G_k = \frac{\#\pi_{\mathfrak{f}}(\mathbb{Z})^*}{\#\mathrm{Ker}(\mu_k)} \geq \frac{\#\pi_{\mathfrak{f}}(\mathbb{Z})^*}{\#\pi_{\mathfrak{p}_k^{e_k}}(\mathbb{Z})^*}. \tag{5.18}$$

In particular, if $k = 1, \cdots, 2A$, then μ_k becomes injective (and so, bijective). Indeed, if $m \pmod{\mathfrak{f}} \in \pi_{\mathfrak{f}}(\mathbb{Z})^*$ belongs to $\mathrm{Ker}(\mu_k)$, then

$$m \equiv 1 \pmod{\mathfrak{p}_\ell^{e_\ell}} \quad \text{for } \ell \neq k \tag{5.19}$$

by (5.17). But, since m is an integer, (5.19) implies

$$m \equiv 1 \pmod{\bar{\mathfrak{p}}_\ell^{e_\ell}} \quad \text{for } \ell \neq k. \tag{5.20}$$

On the other hand, since $\mathfrak{p}_k = \overline{\mathfrak{p}}_{k+A}$ or $\overline{\mathfrak{p}}_{k-A}$ by definition (5.16), we deduce by (5.19) and (5.20) that

$$m \equiv 1 \pmod{\mathfrak{p}_\ell^{e_\ell}} \quad \text{for all } \ell = 1, \cdots, n,$$

from which we get $m \equiv 1 \pmod{\mathfrak{f}}$. This concludes that μ_k is injective; hence

$$\#G_k = \#\pi_{\mathfrak{f}}(\mathbb{Z})^* \quad \text{for } k = 1, \cdots, 2A. \tag{5.21}$$

Thus we achieve by (5.18), (5.21) and the Euler function for integers and ideals that

$$\text{(LHS) of (5.14)} \leq 4\sum_{a=1}^{A} \frac{1}{(s_a - 1)s_a^{u_a - 1}} + 2\sum_{b=1}^{B} \frac{1}{(q_b + 1)q_b^{v_b - 1}} + 2\sum_{c=1}^{C} \frac{1}{r_c^{w_c}}.$$

Therefore, one can also apply Theorem 5.4 under the assumption

$$4\sum_{a=1}^{A} \frac{1}{(s_a - 1)s_a^{u_a - 1}} + 2\sum_{b=1}^{B} \frac{1}{(q_b + 1)q_b^{v_b - 1}} + 2\sum_{c=1}^{C} \frac{1}{r_c^{w_c}} < 1. \tag{5.22}$$

Example 5.6. Let $K = \mathbb{Q}(\sqrt{-2})$ and $\mathcal{O}$ be the order of conductor $N = 9(= 3^2)$ in K. Then $N\mathcal{O}_K$ satisfies the assumption (5.22) in Remark 5.5 (but, not the assumption (2.3) in Lemma 2.5) and hence the singular value $3^{12}\frac{\Delta(9\theta)}{\Delta(3\theta)}$ with $\theta = \sqrt{-2}$ generates $H_\mathcal{O}$ over K by Theorem 5.4. Since $h_K = 1([4])$, one can estimate its minimal polynomial in exactly the same way as the previous examples:

$$\begin{aligned}\min\left(3^{12}\tfrac{\Delta(9\theta)}{\Delta(3\theta)},\ K\right) \;=\;& X^6 + 52079706X^5 + 2739284675932815X^4 + 12787916715651570220X^3\\ &+19073250572430210646 0815X^2 - 268398119546256294X + 1.\end{aligned}$$

References

1. 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.
2. B. Cho and J. K. Koo, *Construction of class fields over imaginary quadratic fields and applications*, Quart. J. Math., doi:10.1093/qmath/han035.
3. H. Cohen, *Advanced Topics in Computational Number Theory*, Springer, 1999.
4. D. A. Cox, *Primes of the form $x^2 + ny^2$: Fermat, Class Field, and Complex Multiplication*, John Wiley & Sons, Inc., 1989.
5. D. A. Cox, J. McKay and P. Stevenhagen, *Principal moduli and class fields*, Bull. London Math. Soc. 36 (2004), no. 1, 3-12.
6. A. Gee, *Class invariants by Shimura's reciprocity law*, J. Theor. Nombres Bordeaux 11 (1999), no. 1, 45-72.
7. G. J. Janusz, *Algebraic Number Fields*, Academic Press, 1973.
8. J. K. Koo and D. H. Shin, *On some arithmetic properties of Siegel functions*, Math. Zeit., DOI 10.1007/s00209-008-0456-9.
9. J. K. Koo and D. H. Shin, *On some ring class invariants over imaginary quadratic fields*, submitted.
10. D. Kubert and S. Lang, *Modular Units*, Grundlehren der mathematischen Wissenschaften 244, Spinger-Verlag, 1981.
11. S. Lang, *Algebraic Number Theory, 2nd edition*, Springer, 1994.
12. S. Lang, *Elliptic Functions, 2nd edition*, Spinger-Verlag, 1987.
13. K. Ramachandra, *Some applications of Kronecker's limit formula*, Ann. of Math. (2) 80(1964), 104-148.
14. R. Schertz, *Construction of ray class fields by elliptic units*, J. Theor. Nombres Bordeaux 9 (1997), no. 2, 383-394.
15. G. Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions*, Iwanami Shoten and Princeton University Press, 1971.
16. P. Stevenhagen, *Hilbert's 12th problem, complex multiplication and Shimura reciprocity*, Class Field Theory-Its Centenary and Prospect (Tokyo, 1998), 161-176, Adv. Stud. Pure Math., 30, Math. Soc. Japan, Tokyo, 2001.

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

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

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