Proceedings of the Royal Society of Edinburgh, **147A**, 781–812, *2017*
DOI:10.1017/S0308210516000263

Construction of ray-class fields by smaller generators and their applications

Ja Kyung Koo and **Dong Sung Yoon**
Department of Mathematical Sciences, Korea Advanced Institute of Science and Technology (KAIST), Daejeon 34141, Republic of Korea
(jkkoo@math.kaist.ac.kr; math_dsyoon@kaist.ac.kr)

(MS received 16 July 2015; accepted 18 December 2015)

We generate ray-class fields over imaginary quadratic fields in terms of Siegel–Ramachandra invariants, which are an extension of a result of Schertz. By making use of quotients of Siegel–Ramachandra invariants we also construct ray-class invariants over imaginary quadratic fields whose minimal polynomials have relatively small coefficients, from which we are able to solve certain quadratic Diophantine equations.

Keywords: class field theory; modular units; Diophantine equations

2010 *Mathematics subject classification:* Primary 11R37; 11G16
Secondary 11Y50

1. Introduction

Let K be an imaginary quadratic field, $\mathfrak{f}$ be a non-zero integral ideal of K and let $\mathrm{Cl}(\mathfrak{f})$ be the ray-class group of K modulo $\mathfrak{f}$. Then, by class field theory, there exists a unique abelian extension of K whose Galois group is isomorphic to $\mathrm{Cl}(\mathfrak{f})$ via the Artin map

$$\sigma\colon \mathrm{Cl}(\mathfrak{f}) \xrightarrow{\sim} \mathrm{Gal}(K_{\mathfrak{f}}/K). \tag{1.1}$$

We call it the *ray-class field* of K modulo $\mathfrak{f}$, which is denoted by $K_{\mathfrak{f}}$. Since any abelian extension of K is contained in some ray-class field $K_{\mathfrak{f}}$, the generation of ray-class fields of K is a key step towards Hilbert's 12th problem. In 1964, Ramachandra [10, theorem 10] constructed a primitive generator of $K_{\mathfrak{f}}$ over K by applying the Kronecker limit formula. However, his invariants involve products of high powers of singular values of Klein forms and the discriminant Delta function, which are quite complicated to use in practice. On the other hand, Schertz tried to find rather simpler generators of $K_{\mathfrak{f}}$ over K for practical use. And he conjectured that the Siegel–Ramachandra invariants would be the right answer and gave a conditional proof (see [11, theorems 3 and 4] or [12, theorem 6.8.4]).

In this paper we shall first generate ray-class fields $K_{\mathfrak{f}}$ over K via Siegel–Ramachandra invariants by improving Schertz's idea (theorem 4.6). By making use of the quotient of Siegel–Ramachandra invariants we shall also construct a primitive generator of $K_{\mathfrak{f}}$ over K whose minimal polynomial has relatively small coefficients, and present several examples (see theorem 5.4, remark 5.6 and examples 5.8 and 5.9). This ray-class invariant becomes a real algebraic integer with certain conditions (see lemma 6.2 and theorem 6.3). Lastly, we shall apply the real ray-class invariant to solving certain quadratic Diophantine equations (see theorem 6.3 and examples 6.6 and 6.7).

Notation. For $z \in \mathbb{C}$ we denote by $\bar{z}$ the complex conjugate of z and by $\mathrm{Im}(z)$ the imaginary part of z, and set $q_z = \mathrm{e}^{2\pi \mathrm{i} z}$. If G is a group and $g_1, g_2, \dots, g_r$ are elements of G, let $\langle g_1, g_2, \dots, g_r \rangle$ be the subgroup of G generated by $g_1, g_2, \dots, g_r$, and let G^n be the subgroup $\{g^n \mid g \in G\}$ of G for $n \in \mathbb{Z}_{>0}$. Moreover, if H is a subgroup of G and $g \in G$, we mean by $[g]$ the coset gH of H in G. The transpose of a matrix α is denoted by ${}^{\mathrm{t}}\alpha$. If R is a ring with identity, $R^\times$ indicates the group of all invertible elements of R. For a number field K, let $\mathcal{O}_K$ be the ring of algebraic integers of K and let d_K be the discriminant of K. If $a \in \mathcal{O}_K$, we denote by (a) the principal ideal of K generated by a. When $\mathfrak{a}$ is an integral ideal of K, we mean by $\mathcal{N}(\mathfrak{a})$ the absolute norm of an ideal $\mathfrak{a}$. For a positive integer N, we let $\zeta_N = \mathrm{e}^{2\pi \mathrm{i}/N}$ be a primitive Nth root of unity.

2. Shimura's reciprocity law

We shall review an algorithm for finding all conjugates of the special value of a modular function over an imaginary quadratic field by using Shimura's reciprocity law.

For a lattice L in $\mathbb{C}$, the *Weierstrass ℘-function* is defined by

$$\wp(z; L) = \frac{1}{z^2} + \sum_{\omega \in L \setminus \{0\}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right) \quad (z \in \mathbb{C}).$$

Let $\mathbb{H} = \{z \in \mathbb{C} \mid \mathrm{Im}(z) > 0\}$ be the complex upper half-plane. For $\tau \in \mathbb{H}$, we let

$$g_2(\tau) = 60 \sum_{\omega \in [\tau,1] \setminus \{0\}} \frac{1}{\omega^4}, \quad g_3(\tau) = 140 \sum_{\omega \in [\tau,1] \setminus \{0\}} \frac{1}{\omega^6}, \quad \Delta(\tau) = g_2(\tau)^3 - 27 g_3(\tau)^2.$$

Then the *j-invariant* is defined by

$$j(\tau) = 1728 \frac{g_2(\tau)}{\Delta(\tau)} \quad (\tau \in \mathbb{H}).$$

For a rational vector $\boldsymbol{r} = \left[\begin{smallmatrix} r_1 \\ r_2 \end{smallmatrix}\right] \in \mathbb{Q}^2 \setminus \mathbb{Z}^2$, we define the *Fricke function* by

$$f_{\boldsymbol{r}}(\tau) = -2^7 3^5 \frac{g_2(\tau) g_3(\tau)}{\Delta(\tau)} \wp(r_1 \tau + r_2; [\tau, 1]) \qquad (\tau \in \mathbb{H}).$$

And, for a positive integer N, let

$$\Gamma(N) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \;\middle|\; \begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \pmod{N} \right\},$$

$$\mathcal{F}_N = \mathbb{Q}\left(j(\tau), f_{\boldsymbol{r}}(\tau) \colon \boldsymbol{r} \in \frac{1}{N}\mathbb{Z}^2 \setminus \mathbb{Z}^2 \right).$$

We call $\mathcal{F}_N$ the *modular function field of level* N over $\mathbb{Q}$. Then the function field $\mathbb{C}(X(N))$ on the modular curve $X(N) = \Gamma(N) \setminus (\mathbb{H} \cup \mathbb{P}^1(\mathbb{Q}))$ is equal to $\mathbb{C}\mathcal{F}_N$, and $\mathcal{F}_N$ consists of all functions in $\mathbb{C}(X(N))$ whose Fourier coefficients lie in the cyclotomic field $\mathbb{Q}(\zeta_N)$ [7, ch. 6, § 3]. As is well known, $\mathcal{F}_N$ is a Galois extension of $\mathcal{F}_1 = \mathbb{Q}(j(\tau))$ and

$$\mathrm{Gal}(\mathcal{F}_N/\mathcal{F}_1) \cong \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I_2\} \cong G_N \cdot \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I_2\}, \tag{2.1}$$

where

$$G_N = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & d \end{bmatrix} \,\middle|\, d \in (\mathbb{Z}/N\mathbb{Z})^\times \right\}.$$

More precisely, the element $\left[\begin{smallmatrix} 1 & 0 \\ 0 & d \end{smallmatrix}\right] \in G_N$ acts on $\mathcal{F}_N$ by

$$\sum_{n \gg -\infty} c_n q_\tau^{n/N} \mapsto \sum_{n \gg -\infty} c_n^{\sigma_d} q_\tau^{n/N}, \tag{2.2}$$

where $\sum_{n \gg -\infty} c_n q_\tau^{n/N}$ is the Fourier expansion of a function in $\mathcal{F}_N$ and $\sigma_d \in \mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$ satisfies $\zeta_N^{\sigma_d} = \zeta_N^d$. And, $\gamma \in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I_2\}$ acts on $h \in \mathcal{F}_N$ by

$$h^\gamma(\tau) = h(\tilde{\gamma}\tau),$$

where $\tilde{\gamma}$ is a preimage of γ of the reduction $\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I_2\}$ [7, ch. 6, theorem 3].

Now let K be an imaginary quadratic field of discriminant d_K and set

$$\theta = \begin{cases} \frac{1}{2}\sqrt{d_K} & \text{if } d_K \equiv 0 \pmod 4, \\ \frac{1}{2}(-1 + \sqrt{d_K}) & \text{if } d_K \equiv 1 \pmod 4, \end{cases} \tag{2.3}$$

so that $\mathcal{O}_K = \mathbb{Z}[\theta]$. Then its minimal polynomial over $\mathbb{Q}$ is

$$\min(\theta, \mathbb{Q}) = X^2 + B_\theta X + C_\theta = \begin{cases} X^2 - \frac{1}{4}d_K & \text{if } d_K \equiv 0 \pmod 4, \\ X^2 + X + \frac{1}{4}(1 - d_K) & \text{if } d_K \equiv 1 \pmod 4. \end{cases}$$

Proposition 2.1. *When $\mathfrak{f} = N\mathcal{O}_K$ for a positive integer N, we have*

$$K_\mathfrak{f} = K_{(N)} = K(h(\theta) \colon h \in \mathcal{F}_{N,\theta}),$$

where $\mathcal{F}_{N,\theta} = \{h \in \mathcal{F}_N \mid h \text{ is defined and finite at } \theta\}$. If $N = 1$, then $K_{(1)}$ is merely the Hilbert class field of K.

Proof. See [7, ch. 10 § 1, corollary]. □

For a positive integer N we define a subgroup $W_{N,\theta}$ of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ by

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

Then we have the following proposition.

Proposition 2.2. *We attain a surjective homomorphism*

$$\varphi_{N,\theta}\colon W_{N,\theta} \to \mathrm{Gal}(K_{(N)}/K_{(1)})$$
$$\alpha \mapsto (h(\theta) \mapsto h^{\alpha}(\theta))_{h\in\mathcal{F}_{N,\theta}},$$

whose kernel is

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

Proof. See [3, § 3] or [16, § 3]. □

On the other hand, observe that the subgroup

$$\{[(\omega)]\in\mathrm{Cl}(N\mathcal{O}_K)\mid \omega\in\mathcal{O}_K \text{ is prime to } N\}$$

is isomorphic to $\mathrm{Gal}(K_{(N)}/K_{(1)})$ via the Artin map σ in (1.1).

Proposition 2.3. *Let N be a positive integer and let $\omega\in\mathcal{O}_K$ be prime to N. Write $\omega=s\theta+t$ with $s,t\in\mathbb{Z}$. Then, for $h\in\mathcal{F}_{N,\theta}$ we obtain*

$$h(\theta)^{\sigma([(\omega)])}=h^{\alpha}(\theta), \quad \textit{where } \alpha=\begin{bmatrix}t-B_\theta s & -C_\theta s\\ s & t\end{bmatrix}\in W_{N,\theta}.$$

Proof. See [14, theorem 6.31]. □

For convenience we denote the quadratic form $aX^2+bXY+cY^2\in\mathbb{Z}[X,Y]$ by $[a,b,c]$. Let $C(d_K)$ be the form class group of discriminant d_K. Then we identify $C(d_K)$ with the set of all *reduced quadratic forms*, namely [2, theorem 2.8]

$$C(d_K)=\{[a,b,c]\in\mathbb{Z}[X,Y]\mid \gcd(a,b,c)=1,\quad b^2-4ac=d_K,$$
$$-a<b\leqslant a<c \text{ or } 0\leqslant b\leqslant a=c\}.$$

Here we note that if $[a,b,c]\in C(d_K)$, then $a\leqslant\sqrt{-d_K/3}$ [2, p. 29] and $C(d_K)$ is isomorphic to $\mathrm{Gal}(K_{(1)}/K)$ [2, theorem 7.7]. For $Q=[a,b,c]\in C(d_K)$, we let

$$\theta_Q=\frac{-b+\sqrt{d_K}}{2a}\in\mathbb{H}.$$

Further, we define $\beta_Q=(\beta_p)_p\in\prod_p \mathrm{GL}_2(\mathbb{Z}_p)$ as follows.

https://doi.org/10.1017/S0308210516000263 Published online by Cambridge University Press

CASE 1 ($d_K \equiv 0 \pmod 4$).

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

CASE 2 ($d_K \equiv 1 \pmod 4$).

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

PROPOSITION 2.4. *For a positive integer N, we achieve a one-to-one correspondence*

$$\begin{aligned} W_{N,\theta}/\ker(\varphi_{N,\theta}) \times C(d_K) &\to \mathrm{Gal}(K_{(N)}/K) \\ (\alpha, Q) &\mapsto (h(\theta) \mapsto h^{\tilde{\alpha}\beta_Q}(\theta_Q))_{h \in \mathcal{F}_{N,\theta}}. \end{aligned}$$

Here, $\tilde{\alpha}$ is the preimage of α of the reduction

$$W_{N,\theta}/\{\pm I_2\} \to W_{N,\theta}/\ker(\varphi_{N,\theta})$$

and the action of β_Q on $\mathcal{F}_N$ is described by the action of $\beta \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I_2\}$ so that $\beta \equiv \beta_p \pmod{N\mathbb{Z}_p}$ for all primes $p|N$.

Proof. This is immediate from proposition 2.2 and [3, § 4]. □

3. Siegel–Ramachandra invariants

In this section we introduce the arithmetic properties of Siegel functions and describe some necessary facts about Siegel–Ramachandra invariants for later use.

For a rational vector $\boldsymbol{r} = \left[\begin{smallmatrix} r_1 \\ r_2 \end{smallmatrix}\right] \in \mathbb{Q}^2 \setminus \mathbb{Z}^2$, we define the *Siegel function* $g_{\boldsymbol{r}}(\tau)$ on $\mathbb{H}$ by the following infinite product:

$$g_{\boldsymbol{r}}(\tau) = -q_\tau^{\boldsymbol{B}_2(r_1)/2} \mathrm{e}^{\pi \mathrm{i} r_2(r_1-1)}(1 - q_\tau^{r_1}\mathrm{e}^{2\pi \mathrm{i} r_2}) \prod_{n=1}^{\infty}(1 - q_\tau^{n+r_1}\mathrm{e}^{2\pi \mathrm{i} r_2})(1 - q_\tau^{n-r_1}\mathrm{e}^{-2\pi \mathrm{i} r_2}),$$

where $\boldsymbol{B}_2(X) = X^2 - X + \frac{1}{6}$ is the second Bernoulli polynomial. Then it has no zeros and poles on $\mathbb{H}$ (see [15] or [6, p. 36]). The following proposition describes the modularity criterion for Siegel functions.

Proposition 3.1. *Let $N \geqslant 2$ be a positive integer and let $\{m(\boldsymbol{r})\}_{\boldsymbol{r}=\left[\begin{smallmatrix} r_1 \\ r_2 \end{smallmatrix}\right] \in (1/N)\mathbb{Z}^2 \setminus \mathbb{Z}^2}$ be a family of integers such that $m(\boldsymbol{r}) = 0$ except for finitely many $\boldsymbol{r}$. A finite product of Siegel functions*

$$\zeta \prod_{\boldsymbol{r} \in (1/N)\mathbb{Z}^2 \setminus \mathbb{Z}^2} g_{\boldsymbol{r}}(\tau)^{m(\boldsymbol{r})}$$

belongs to $\mathcal{F}_N$ if

$$\sum_{\boldsymbol{r}} m(\boldsymbol{r})(Nr_1)^2 \equiv \sum_{\boldsymbol{r}} m(\boldsymbol{r})(Nr_2)^2 \equiv 0 \pmod{\gcd(2, N) \cdot N},$$

$$\sum_{\boldsymbol{r}} m(\boldsymbol{r})(Nr_1)(Nr_2) \equiv 0 \pmod{N},$$

$$\sum_{\boldsymbol{r}} m(\boldsymbol{r}) \cdot \gcd(12, N) \equiv 0 \pmod{12}.$$

Here,

$$\zeta = \prod_{\boldsymbol{r}} \mathrm{e}^{\pi \mathrm{i} r_2(1-r_1)m(\boldsymbol{r})} \in \mathbb{Q}(\zeta_{2N^2}).$$

Proof. See [6, ch. 3, theorems 5.2 and 5.3]. □

Proposition 3.2. *Let $\boldsymbol{r}, \boldsymbol{s} \in (1/N)\mathbb{Z}^2 \setminus \mathbb{Z}^2$ for a positive integer $N \geqslant 2$.*

(i) *$g_{\boldsymbol{r}}(\tau)^{12N}$ satisfies the relation*

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

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

$$\langle \boldsymbol{r} \rangle = \begin{bmatrix} \langle r_1 \rangle \\ \langle r_2 \rangle \end{bmatrix}.$$

(ii) *$g_{\boldsymbol{r}}(\tau)^{12N}$ belongs to $\mathcal{F}_N$. Moreover, $\alpha \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I_2\}$ acts on it by*

$$(g_{\boldsymbol{r}}(\tau)^{12N})^{\alpha} = g_{{}^{\mathrm{t}}\alpha \boldsymbol{r}}(\tau)^{12N}.$$

(iii) *For $\gamma = \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \in \mathrm{SL}_2(\mathbb{Z})$ we have*

$$\left(\frac{g_{\boldsymbol{r}}(\tau)}{g_{\boldsymbol{s}}(\tau)}\right) \circ \gamma = \frac{g_{{}^{t}\gamma \boldsymbol{r}}(\tau)}{g_{{}^{t}\gamma \boldsymbol{s}}(\tau)}.$$

Proof. See [6, ch. 2, § 1]. □

Let L be a lattice in $\mathbb{C}$ and let $t \in \mathbb{C} \setminus L$ be a point of finite order with respect to L. We choose a basis $[\omega_1, \omega_2]$ of L such that $z = \omega_1/\omega_2 \in \mathbb{H}$ and write

$$t = r_1\omega_1 + r_2\omega_2 \quad \text{for some } \begin{bmatrix} r_1 \\ r_2 \end{bmatrix} \in \mathbb{Q}^2 \setminus \mathbb{Z}^2.$$

We also define a function $g(t, [\omega_1, \omega_2]) = g_{\left[\begin{smallmatrix} r_1 \\ r_2 \end{smallmatrix}\right]}(z)$, which depends on the choice of ω_1, ω_2. However, by raising it to the 12th power we obtain a function $g^{12}(t, L)$ of t and L [6, p. 31].

Now let K be an imaginary quadratic field of discriminant d_K, let $\mathfrak{f}$ be a non-trivial proper integral ideal of K and let N be the smallest positive integer in $\mathfrak{f}$. For $C \in \mathrm{Cl}(\mathfrak{f})$, we define the *Siegel–Ramachandra invariant* of conductor $\mathfrak{f}$ at C by

$$g_{\mathfrak{f}}(C) = g^{12N}(1, \mathfrak{f}\mathfrak{c}^{-1}),$$

where $\mathfrak{c}$ is any integral ideal in C. This value depends only on $\mathfrak{f}$ and the class C, and not on the choice of $\mathfrak{c}$.

PROPOSITION 3.3. *Let $C, C' \in \mathrm{Cl}(\mathfrak{f})$ with $\mathfrak{f} \neq \mathcal{O}_K$.*

(i) *$g_{\mathfrak{f}}(C)$ lies in $K_{\mathfrak{f}}$ as an algebraic integer. If N is composite, $g_{\mathfrak{f}}(C)$ is a unit in $K_{\mathfrak{f}}$.*

(ii) *We have the transformation formula*

$$g_{\mathfrak{f}}(C)^{\sigma(C')} = g_{\mathfrak{f}}(CC'),$$

where σ is the Artin map stated in (1.1).

(iii) *$g_{\mathfrak{f}}(C')/g_{\mathfrak{f}}(C)$ is a unit in $K_{\mathfrak{f}}$.*

Proof. See [7, ch. 19, theorem 3] and [6, ch. 11, theorem 1.2]. □

Further, we let $\mathfrak{a}$ be an integral ideal of K that is not divisible by $\mathfrak{f}$. For a class $C \in \mathrm{Cl}(\mathfrak{f})$, we define the *Robert invariant* by

$$u_{\mathfrak{a}}(C) = \frac{g^{12}(1, \mathfrak{f}\mathfrak{c}^{-1})^{\mathcal{N}(\mathfrak{a})}}{g^{12}(1, \mathfrak{f}\mathfrak{a}^{-1}\mathfrak{c}^{-1})},$$

where $\mathfrak{c}$ is any integral ideal in C. This depends only on the class C. Note that $u_{\mathfrak{a}}(C)$ belongs to $K_{\mathfrak{f}}$, but it is not necessarily a unit [6, ch. 11, theorem 4.1]. We shall take products of such invariants with a linear condition in order to get units. Let C_0 be the unit class in $\mathrm{Cl}(\mathfrak{f})$, and let $\mathfrak{R}_{\mathfrak{f}}^*$ be the group of all finite products

$$\prod_{\mathfrak{a}} u_{\mathfrak{a}}(C_0)^{m(\mathfrak{a})} \quad (m(\mathfrak{a}) \in \mathbb{Z})$$

taken with all integral ideals $\mathfrak{a}$ of K prime to $6N$ satisfying $\sum_{\mathfrak{a}} m(\mathfrak{a})(\mathcal{N}(\mathfrak{a}) - 1) = 0$. Then $\mathfrak{R}_{\mathfrak{f}}^*$ becomes a subgroup of the units in $K_{\mathfrak{f}}$ [6, ch. 11, theorem 4.2].

Let $\omega_{K_{\mathfrak{f}}}$ be the number of roots of unity in $K_{\mathfrak{f}}$, and define the group

$$\Phi_{\mathfrak{f}}(\omega_{K_{\mathfrak{f}}}) = \left\{ \prod_{C \in \mathrm{Cl}(\mathfrak{f})} g_{\mathfrak{f}}(C)^{n(C)} \;\middle|\; \sum_{C} n(C) = 0 \right. \\ \left. \text{and } \sum_{C} n(C)\mathcal{N}(\mathfrak{a}_C) \equiv 0 \pmod{\omega_{K_{\mathfrak{f}}}} \right\},$$

where $\mathfrak{a}_C$ is any integral ideal in C prime to $6N$ and the exponents $n(C)$ are integers. The value $\mathcal{N}(\mathfrak{a}_C) \pmod{\omega_{K_{\mathfrak{f}}}}$ does not depend on the choice of $\mathfrak{a}_C$ [6, ch. 9, lemma 4.1], and so the group is well defined.

Proposition 3.4. *We have*

$$(\mathfrak{R}_{\mathfrak{f}}^{*})^{N} = \Phi_{\mathfrak{f}}(\omega_{K_{\mathfrak{f}}}).$$

Proof. See [6, ch. 11, theorem 4.3] □

Lemma 3.5. *Let* $\mathfrak{f} = N\mathcal{O}_K$ *for a positive integer* $N \geqslant 2$ *and let* C' *be an element of* $\mathrm{Cl}(\mathfrak{f})$ *satisfying* $\mathcal{N}(\mathfrak{a}_{C'}) \equiv 1 \pmod{\omega_{K_{\mathfrak{f}}}}$ *for some integral ideal* $\mathfrak{a}_{C'}$ *in* C' *prime to* $6N$. *Then any* N*th root of the value* $g_{\mathfrak{f}}(C')/g_{\mathfrak{f}}(C_0)$ *is a unit in* $K_{\mathfrak{f}}$.

Proof. Observe that $g_{\mathfrak{f}}(C')/g_{\mathfrak{f}}(C_0) \in \Phi_{\mathfrak{f}}(\omega_{K_{\mathfrak{f}}})$. It then follows from proposition 3.4 that

$$\frac{g_{\mathfrak{f}}(C')}{g_{\mathfrak{f}}(C_0)} = u^N \quad \text{for some } u \in \mathfrak{R}_{\mathfrak{f}}^{*}.$$

Since u is a unit in $K_{\mathfrak{f}}$ and $\zeta_N \in \mathbb{Q}(\zeta_N) \subset K_{(N)} = K_{\mathfrak{f}}$, any Nth root of the value $g_{\mathfrak{f}}(C')/g_{\mathfrak{f}}(C_0)$ is also a unit in $K_{\mathfrak{f}}$. □

Let $\mathfrak{f}$ be a non-trivial integral ideal of K and χ be a character of $\mathrm{Cl}(\mathfrak{f})$. The conductor of χ is defined by the largest ideal $\mathfrak{g}$ dividing $\mathfrak{f}$ such that χ is obtained by a composition of a character of $\mathrm{Cl}(\mathfrak{g})$ and the natural homomorphism $\mathrm{Cl}(\mathfrak{f}) \to \mathrm{Cl}(\mathfrak{g})$, and we denote it by $\mathfrak{f}_\chi$. Similarly, if χ' is a character of $(\mathcal{O}_K/\mathfrak{f})^\times$, then we define the conductor of χ' by the largest ideal $\mathfrak{g}$ dividing $\mathfrak{f}$ for which χ' is induced by a composition of a character of $(\mathcal{O}_K/\mathfrak{g})^\times$ with the natural homomorphism $(\mathcal{O}_K/\mathfrak{f})^\times \to (\mathcal{O}_K/\mathfrak{g})^\times$, and denote it by $\mathfrak{f}_{\chi'}$. The map

$$\begin{aligned} (\mathcal{O}_K/\mathfrak{f})^\times &\to \mathrm{Cl}(\mathfrak{f}) \\ \alpha + \mathfrak{f} &\mapsto [(\alpha)] \end{aligned} \tag{3.1}$$

is a well-defined homomorphism whose kernel is

$$\{\alpha + \mathfrak{f} \in (\mathcal{O}_K/\mathfrak{f})^\times \mid \alpha \in \mathcal{O}_K^\times\}.$$

For a character χ of $\mathrm{Cl}(\mathfrak{f})$, we derive a character χ' of $(\mathcal{O}_K/\mathfrak{f})^\times$ by composing with the map (3.1). Then, by definition, $\mathfrak{f}_\chi = \mathfrak{f}_{\chi'}$ is immediate.

Now let χ be a non-trivial character of $\mathrm{Cl}(\mathfrak{f})$ with $\mathfrak{f} \neq \mathcal{O}_K$ and let χ_0 be the primitive character of $\mathrm{Cl}(\mathfrak{f}_\chi)$ corresponding to χ. We define the *Stickelberger element* and the *L-function* for χ by

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

$$L_{\mathfrak{f}}(s, \chi) = \sum_{\substack{(0) \neq \mathfrak{a} \subset \mathcal{O}_K \\ \gcd(\mathfrak{a}, \mathfrak{f}) = 1}} \frac{\chi(\mathfrak{a})}{\mathcal{N}(\mathfrak{a})^s} \quad (s \in \mathbb{C}),$$

respectively. The second Kronecker limit formula explains the relation between the Stickelberger element and the L-function as follows.

Proposition 3.6. *Let χ be a non-trivial character of* $\mathrm{Cl}(\mathfrak{f})$ *with* $\mathfrak{f}_\chi \neq \mathcal{O}_K$*. Then we have*

$$L_{\mathfrak{f}_\chi}(1,\chi_0)\prod_{\substack{\mathfrak{p}\mid\mathfrak{f}\\ \mathfrak{p}\nmid\mathfrak{f}_\chi}}(1-\bar{\chi}_0([\mathfrak{p}])) = -\frac{2\pi\chi_0([\gamma\mathfrak{d}_K\mathfrak{f}_\chi])}{6N(\mathfrak{f}_\chi)\omega(\mathfrak{f}_\chi)T_\gamma(\bar{\chi}_0)\sqrt{-d_K}}\cdot S_{\mathfrak{f}}(\bar{\chi},g_{\mathfrak{f}}),$$

where $\mathfrak{d}_K$ *is the different ideal of* $K/\mathbb{Q}$*,* γ *is an element of* K *such that* $\gamma\mathfrak{d}_K\mathfrak{f}_\chi$ *is an integral ideal of* K *prime to* $\mathfrak{f}_\chi$*,* $N(\mathfrak{f}_\chi)$ *is the smallest positive integer in* $\mathfrak{f}_\chi$*,* $\omega(\mathfrak{f}_\chi)$ *is the number of roots of unity in* K *that are* $\equiv 1 \pmod{\mathfrak{f}_\chi}$ *and*

$$T_\gamma(\bar{\chi}_0) = \sum_{x+\mathfrak{f}_\chi\in(\mathcal{O}_K/\mathfrak{f}_\chi)^\times}\bar{\chi}_0([x\mathcal{O}_K])\mathrm{e}^{2\pi\mathrm{i}\,\mathrm{Tr}_{K/\mathbb{Q}}(\gamma x)}.$$

Proof. See [6, ch. 11, § 2, LF2]. □

Remark 3.7. Since χ_0 is a non-trivial character of $\mathrm{Cl}(\mathfrak{f}_\chi)$, we obtain $L_{\mathfrak{f}_\chi}(1,\chi_0)\neq 0$ [4, ch. V, theorem 10.2]. Furthermore, the Gauss sum $T_\gamma(\bar{\chi}_0)$ is also non-zero [7, ch. 22, § 1, G3]. If every prime ideal factor of $\mathfrak{f}$ divides $\mathfrak{f}_\chi$, then we understand the Euler factor $\prod_{\mathfrak{p}\mid\mathfrak{f},\ \mathfrak{p}\nmid\mathfrak{f}_\chi}(1-\bar{\chi}_0([\mathfrak{p}]))$ to be 1, and hence we conclude that $S_{\mathfrak{f}}(\bar{\chi},g_{\mathfrak{f}})\neq 0$.

4. Generation of ray-class fields by Siegel–Ramachandra invariants

In this section we improve the result of Schertz [12] concerning construction of ray-class fields by means of Siegel–Ramachandra invariants.

Let K be an imaginary quadratic field of discriminant d_K and let ω_K be the number of roots of unity in K. For a non-trivial integral ideal $\mathfrak{f}$ of K, we regard $\omega(\mathfrak{f})$ as the number of roots of unity in K that are equivalent to $1 \pmod{\mathfrak{f}}$. Let ϕ be the Euler function for ideals, namely

$$\phi(\mathfrak{f}) = |(\mathcal{O}_K/\mathfrak{f})^\times| = \mathcal{N}(\mathfrak{f})\prod_{\substack{\mathfrak{p}\mid\mathfrak{f}\\ \mathfrak{p}\ \text{prime}}}\left(1-\frac{1}{\mathcal{N}(\mathfrak{p})}\right). \tag{4.1}$$

Proposition 4.1. *If* $\mathfrak{f}$ *is a non-trivial integral ideal of* K*, then we get*

$$[K_{\mathfrak{f}}:K] = h_K\phi(\mathfrak{f})\frac{\omega(\mathfrak{f})}{\omega_K},$$

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

Proof. See [8, ch. VI, theorem 1]. □

Lemma 4.2. *Let* $H\subset G$ *be two finite abelian groups, let* $g\in G\setminus H$ *and* n *be the order of the coset* $[g]$ *in* G/H*. Then for any character* χ *of* H*, we can extend it to a character* ψ *of* G *such that* $\psi(g)$ *is any fixed nth root of* $\chi(g^n)$*.*

Proof. See [13, ch. VI, proposition 1]. □

Now, let $\mathfrak{f}$ be a non-trivial proper integral ideal of K with prime ideal factorization

$$\mathfrak{f} = \prod_{i=1}^{r}\mathfrak{p}_i^{n_i},$$

and let C_0 be the unit class in $\mathrm{Cl}(\mathfrak{f})$. Consider the quotient group

$$\boldsymbol{G} = (\mathcal{O}_K/\mathfrak{f})^\times / \{\alpha + \mathfrak{f} \in (\mathcal{O}_K/\mathfrak{f})^\times \mid \alpha \in \mathcal{O}_K^\times\}.$$

Then one can view $\boldsymbol{G}$ as a subgroup of $\mathrm{Cl}(\mathfrak{f})$ via the map (3.1). For each i, we set

$$\boldsymbol{G}_i = (\mathcal{O}_K/\mathfrak{p}_i^{n_i})^\times / \{\alpha + \mathfrak{p}_i^{n_i} \in (\mathcal{O}_K/\mathfrak{p}_i^{n_i})^\times \mid \alpha \in \mathcal{O}_K^\times\}.$$

Proposition 4.3. *Assume that* $|\boldsymbol{G}_i| > 2$ *for every* i. *Then, for any class* $C\,(\neq C_0) \in \mathrm{Cl}(\mathfrak{f})$ *there exists a character* χ *of* $\mathrm{Cl}(\mathfrak{f})$ *such that* $\chi(C) \neq 1$ *and* $\mathfrak{p}_i | \mathfrak{f}_\chi$ *for all* i.

Proof. Since $C \neq C_0$, there is a character χ of $\mathrm{Cl}(\mathfrak{f})$ such that $\chi(C) \neq 1$. We set n to be the order of C in the quotient group $\mathrm{Cl}(\mathfrak{f})/\boldsymbol{G}$. Then $C^n = [(\beta)]$ for some $\beta \in \mathcal{O}_K$ that is relatively prime to $\mathfrak{f}$. Suppose that $\mathfrak{f}_\chi$ is not divided by $\mathfrak{p}_i$ for some i. If $\boldsymbol{G}_i \neq \langle \beta + \mathfrak{p}_i^{n_i} \rangle$, then we can find a non-trivial character ψ of $(\mathcal{O}_K/\mathfrak{p}_i^{n_i})^\times$ for which ψ is trivial on $\{\alpha + \mathfrak{p}_i^{n_i} \in (\mathcal{O}_K/\mathfrak{p}_i^{n_i})^\times \mid \alpha \in \mathcal{O}_K^\times\}$ and $\psi(\beta + \mathfrak{p}_i^{n_i}) = 1$. By composing with a natural homomorphism $(\mathcal{O}_K/\mathfrak{f})^\times \to (\mathcal{O}_K/\mathfrak{p}_i^{n_i})^\times$, we are able to extend ψ to a character ψ' of $(\mathcal{O}_K/\mathfrak{f})^\times$ whose conductor is divisible only by $\mathfrak{p}_i$. Observe that ψ' is trivial on $\{\alpha + \mathfrak{f} \in (\mathcal{O}_K/\mathfrak{f})^\times \mid \alpha \in \mathcal{O}_K^\times\}$, and so ψ' becomes a character of $\boldsymbol{G}$. It then follows from lemma 4.2 that we can also extend ψ' to a character ψ'' of $\mathrm{Cl}(\mathfrak{f})$ such that $\psi''(C) = 1$. Now assume that $\boldsymbol{G}_i = \langle \beta + \mathfrak{p}_i^{n_i} \rangle$. Since $|\boldsymbol{G}_i| > 2$, there is a non-trivial character ψ of $(\mathcal{O}_K/\mathfrak{p}_i^{n_i})^\times$ such that ψ is trivial on $\{\alpha + \mathfrak{p}_i^{n_i} \in (\mathcal{O}_K/\mathfrak{p}_i^{n_i})^\times \mid \alpha \in \mathcal{O}_K^\times\}$ and $\psi(\beta + \mathfrak{p}_i^{n_i}) \neq 1,\ \chi(C^n)^{-1}$. In a similar way, one can extend ψ to a character ψ'' of $\mathrm{Cl}(\mathfrak{f})$ in such a way that $\mathfrak{f}_{\psi''}$ is divisible only by $\mathfrak{p}_i$ and $\psi''(C) \neq \chi(C)^{-1}$. Therefore, the character $\chi\psi''$ of $\mathrm{Cl}(\mathfrak{f})$ satisfies $\chi\psi''(C) \neq 1$, $\mathfrak{p}_i | \mathfrak{f}_{\chi\psi''}$ and $\mathfrak{f}_\chi | \mathfrak{f}_{\chi\psi''}$ in both cases. By continuing this process for all i, we finally obtain the desired character. □

Lemma 4.4. *With the notation above,* $|\boldsymbol{G}_i| = 1, 2$ *if and only if* $\mathfrak{p}_i^{n_i}$ *satisfies one of the following conditions.*

Case 1 ($K \neq \mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-3})$).

- 2 is not inert in K, $\mathfrak{p}_i$ is lying over 2 and $n_i = 1, 2$ or 3.
- 3 is not inert in K, $\mathfrak{p}_i$ is lying over 3 and $n_i = 1$.
- 5 is not inert in K, $\mathfrak{p}_i$ is lying over 5 and $n_i = 1$.

Case 2 ($K = \mathbb{Q}(\sqrt{-1})$).

- $\mathfrak{p}_i$ is lying over 2 and $n_i = 1, 2, 3$ or 4.
- $\mathfrak{p}_i$ is lying over 3 and $n_i = 1$.
- $\mathfrak{p}_i$ is lying over 5 and $n_i = 1$.

Case 3 ($K = \mathbb{Q}(\sqrt{-3})$).

- $\mathfrak{p}_i$ is lying over 2 and $n_i = 1$ or 2.
- $\mathfrak{p}_i$ is lying over 3 and $n_i = 1$ or 2.

https://doi.org/10.1017/S0308210516000263 Published online by Cambridge University Press

- $\mathfrak{p}_i$ is lying over 7 and $n_i = 1$.

- $\mathfrak{p}_i$ is lying over 13 and $n_i = 1$.

Proof. First, we note that

$$|\boldsymbol{G}_i| = \phi(\mathfrak{p}_i^{n_i})\frac{\omega(\mathfrak{p}_i^{n_i})}{\omega_K}. \tag{4.2}$$

Let p_i be a prime number such that $\mathfrak{p}_i$ is lying over p_i. It then follows from (4.1) that

$$\phi(\mathfrak{p}_i^{n_i}) = \begin{cases} p_i^{2n_i} - p_i^{2n_i-2} & \text{if } p_i \text{ is inert in } K, \\ p_i^{n_i} - p_i^{n_i-1} & \text{otherwise.} \end{cases} \tag{4.3}$$

If $K \neq \mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-3})$, then $\omega_K = 2$ and

$$\omega(\mathfrak{p}_i^{n_i}) = \begin{cases} 2 & \text{if } \mathfrak{p}_i^{n_i} | 2\mathcal{O}_K, \\ 1 & \text{otherwise.} \end{cases} \tag{4.4}$$

If $K = \mathbb{Q}(\sqrt{-1})$, then $\omega_K = 4$ and

$$\left(\frac{d_K}{p_i}\right) = \left(\frac{-4}{p_i}\right) = \begin{cases} 1 & \text{if } p_i \equiv 1 \pmod 4, \\ -1 & \text{if } p_i \equiv 3 \pmod 4, \\ 0 & \text{if } p_i = 2, \end{cases} \tag{4.5}$$

where (d_K/p_i) stands for the Kronecker symbol. Since $2\mathcal{O}_K = (1-\sqrt{-1})^2\mathcal{O}_K$, we deduce that

$$\omega(\mathfrak{p}_i^{n_i}) = \begin{cases} 4 & \text{if } \mathfrak{p}_i^{n_i} = (1-\sqrt{-1})\mathcal{O}_K, \\ 2 & \text{if } \mathfrak{p}_i^{n_i} \neq (1-\sqrt{-1})\mathcal{O}_K \text{ and } \mathfrak{p}_i^{n_i} | 2\mathcal{O}_K, \\ 1 & \text{otherwise.} \end{cases} \tag{4.6}$$

If $K = \mathbb{Q}(\sqrt{-3})$, then $\omega_K = 6$ and

$$\left(\frac{d_K}{p_i}\right) = \left(\frac{-3}{p_i}\right) = \begin{cases} 1 & \text{if } p_i \equiv 1, 7 \pmod{12}, \\ -1 & \text{if } p_i \equiv 5, 11 \pmod{12} \text{ or } p_i = 2, \\ 0 & \text{if } p_i = 3. \end{cases} \tag{4.7}$$

Here we observe that 2 is inert in K and 3 is ramified in K, so to speak: $3\mathcal{O}_K = (\frac{1}{2}(3+\sqrt{-3}))^2\mathcal{O}_K$. One can then readily show that

$$\omega(\mathfrak{p}_i^{n_i}) = \begin{cases} 3 & \text{if } \mathfrak{p}_i^{n_i} = (\frac{1}{2}(3+\sqrt{-3}))\mathcal{O}_K, \\ 2 & \text{if } \mathfrak{p}_i^{n_i} = 2\mathcal{O}_K, \\ 1 & \text{otherwise.} \end{cases} \tag{4.8}$$

Therefore, the lemma follows from (4.2)–(4.8). □

Remark 4.5. If 2 is not inert in K, $\mathfrak{p}_i$ is lying over 2 and $n_i = 1$, then

$$K_{\mathfrak{f}} = K_{\mathfrak{f}\mathfrak{p}_i^{-n_i}}.$$

Indeed, we see from proposition 4.1 that

$$[K_{\mathfrak{f}\mathfrak{p}_i^{-n_i}}:K] = \frac{\omega(\mathfrak{f}\mathfrak{p}_i^{-n_i})}{\phi(\mathfrak{p}_i^{n_i})\omega(\mathfrak{f})} \cdot [K_{\mathfrak{f}}:K]. \tag{4.9}$$

Since $\phi(\mathfrak{p}_i^{n_i}) = 1$ and $\omega(\mathfrak{f}\mathfrak{p}_i^{-n_i}) = \omega(\mathfrak{f})$ in this case, we obtain the conclusion.

From now on we assume that $K_{\mathfrak{f}} \neq K_{\mathfrak{f}\mathfrak{p}_i^{-n_i}}$ for every i and let $\boldsymbol{N}_{\mathfrak{f}}$ be the number of i such that $|G_i| = 1$ or 2. After reordering prime ideal factors of $\mathfrak{f}$ if necessary, we may suppose that $|G_i| = 1$ or 2 for $i = 1, 2, \ldots, \boldsymbol{N}_{\mathfrak{f}}$. For any intermediate field F of the extension $K_{\mathfrak{f}}/K$ we mean 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 σ stated in (1.1).

Theorem 4.6. *Let $\mathfrak{f}$ be a non-trivial proper integral ideal of K with prime ideal factorization $\mathfrak{f} = \prod_{i=1}^{r} \mathfrak{p}_i^{n_i}$ such that $|\boldsymbol{G}_i| = 1$ or 2 for $i = 1, 2, \ldots, \boldsymbol{N}_{\mathfrak{f}}$. Assume that $K_{\mathfrak{f}} \neq K_{\mathfrak{f}\mathfrak{p}_i^{-n_i}}$ for every i and*

$$\sum_{i=1}^{\boldsymbol{N}_{\mathfrak{f}}} \frac{1}{\phi(\mathfrak{p}_i^{n_i})} \leqslant \frac{1}{2}. \tag{4.10}$$

Then, for any class $C \in \mathrm{Cl}(\mathfrak{f})$ and any non-zero integer n, we get

$$K_{\mathfrak{f}} = K(g_{\mathfrak{f}}(C)^n). \tag{4.11}$$

In particular, if $\boldsymbol{N}_{\mathfrak{f}} = 0$ or 1, then the assumption (4.10) is always satisfied, and hence we have the desired result, (4.11).

Proof. Let $F = K(g_{\mathfrak{f}}(C_0)^n)$. On the contrary suppose that F is properly contained in $K_{\mathfrak{f}}$, i.e. $\mathrm{Cl}(K_{\mathfrak{f}}/F) \neq \{1\}$. Then we claim that there exists a character χ of $\mathrm{Cl}(\mathfrak{f})$ satisfying $\chi|_{\mathrm{Cl}(K_{\mathfrak{f}}/F)} \neq 1$ and $\mathfrak{p}_i | \mathfrak{f}_\chi$ for $i = 1, 2, \ldots, \boldsymbol{N}_{\mathfrak{f}}$. Indeed, we deduce that

$$\begin{aligned} M_1 &= |\{\text{characters } \chi \text{ of } \mathrm{Cl}(\mathfrak{f}) \mid \chi|_{\mathrm{Cl}(K_{\mathfrak{f}}/F)} \neq 1\}| \\ &= |\{\text{characters } \chi \text{ of } \mathrm{Cl}(\mathfrak{f})\}| - |\{\text{characters } \chi \text{ of } \mathrm{Cl}(\mathfrak{f}) \mid \chi|_{\mathrm{Cl}(K_{\mathfrak{f}}/F)} = 1\}| \\ &= [K_{\mathfrak{f}}:K] - [F:K] \\ &= [K_{\mathfrak{f}}:K]\left(1 - \frac{1}{[K_{\mathfrak{f}}:F]}\right) \\ &\geqslant \tfrac{1}{2}[K_{\mathfrak{f}}:K]. \end{aligned} \tag{4.12}$$

Thus, if $\boldsymbol{N}_{\mathfrak{f}} = 0$, the claim is clear. Observe that a trivial character is not contained in the set stated in (4.12). Now assume $\boldsymbol{N}_{\mathfrak{f}} \geqslant 1$ and let

$$M_2 = |\{\text{characters } \chi \neq 1 \text{ of } \mathrm{Cl}(\mathfrak{f}) \mid \mathfrak{p}_i \nmid \mathfrak{f}_\chi \text{ for some } i \in \{1, 2, \ldots, \boldsymbol{N}_{\mathfrak{f}}\}\}|.$$

https://doi.org/10.1017/S0308210516000263 Published online by Cambridge University Press

First, we suppose $\boldsymbol{N}_{\mathfrak{f}} \neq 2$. Then we derive that

$$\begin{aligned} M_2 &= |\{\text{characters } \chi \text{ of } \mathrm{Cl}(\mathfrak{f}) \mid \mathfrak{p}_i \nmid \mathfrak{f}_\chi \text{ for some } i \in \{1,2,\ldots,\boldsymbol{N}_{\mathfrak{f}}\}\}| - 1 \\ &= |\{\text{characters } \chi \text{ of } \mathrm{Cl}(\mathfrak{f}) \mid \mathfrak{f}_\chi | \mathfrak{f}\mathfrak{p}_i^{-n_i} \text{ for some } i \in \{1,2,\ldots,\boldsymbol{N}_{\mathfrak{f}}\}\}| - 1 \\ &\leqslant \sum_{i=1}^{\boldsymbol{N}_{\mathfrak{f}}} |\{\text{characters } \chi \text{ of } \mathrm{Cl}(\mathfrak{f}\mathfrak{p}_i^{-n_i})\}| - 1 \\ &= \sum_{i=1}^{\boldsymbol{N}_{\mathfrak{f}}} [K_{\mathfrak{f}\mathfrak{p}_i^{-n_i}} : K] - 1 \\ &= \biggl(\sum_{i=1}^{\boldsymbol{N}_{\mathfrak{f}}} \frac{\omega(\mathfrak{f}\mathfrak{p}_i^{-n_i})}{\phi(\mathfrak{p}_i^{n_i})\omega(\mathfrak{f})}\biggr)[K_{\mathfrak{f}} : K] - 1 \quad (\text{by } (4.9)). \end{aligned}$$

If $\boldsymbol{N}_{\mathfrak{f}} = 1$, then $M_2 \leqslant \frac{1}{2}[K_{\mathfrak{f}} : K] - 1$ since $K_{\mathfrak{f}} \neq K_{\mathfrak{f}\mathfrak{p}_i^{-n_i}}$ for every i. And, if $\boldsymbol{N}_{\mathfrak{f}} \geqslant 3$, then $\omega(\mathfrak{f}) = \omega(\mathfrak{f}\mathfrak{p}_i^{-n_i}) = 1$ for every i because $\mathfrak{f}$ has at least three prime ideal factors. Hence, we attain $M_2 \leqslant \frac{1}{2}[K_{\mathfrak{f}} : K] - 1$, again by the assumption (4.10). Now, assume $\boldsymbol{N}_{\mathfrak{f}} = 2$. Since $\mathfrak{f}$ has at least two prime ideal factors, we obtain that

$$\begin{aligned} M_2 &= |\{\text{characters } \chi \text{ of } \mathrm{Cl}(\mathfrak{f}) \mid \mathfrak{f}_\chi | \mathfrak{f}\mathfrak{p}_i^{-n_i} \text{ for some } i \in \{1,2\}\}| - 1 \\ &= \sum_{i=1}^{2} |\{\text{characters } \chi \text{ of } \mathrm{Cl}(\mathfrak{f}\mathfrak{p}_i^{-n_i})\}| - |\{\text{characters } \chi \text{ of } \mathrm{Cl}(\mathfrak{f}\mathfrak{p}_1^{-n_1}\mathfrak{p}_2^{-n_2})\}| - 1 \\ &= \sum_{i=1}^{2} [K_{\mathfrak{f}\mathfrak{p}_i^{-n_i}} : K] - [K_{\mathfrak{f}\mathfrak{p}_1^{-n_1}\mathfrak{p}_2^{-n_2}} : K] - 1 \\ &= \biggl(\sum_{i=1}^{2} \frac{\omega(\mathfrak{f}\mathfrak{p}_i^{-n_i})}{\phi(\mathfrak{p}_i^{n_i})} - \frac{\omega(\mathfrak{f}\mathfrak{p}_1^{-n_1}\mathfrak{p}_2^{-n_2})}{\phi(\mathfrak{p}_1^{n_1})\phi(\mathfrak{p}_2^{n_2})}\biggr)[K_{\mathfrak{f}} : K] - 1. \end{aligned}$$

Here we note that $\omega(\mathfrak{f}\mathfrak{p}_i^{-n_i}) \neq 1$ occurs only when $\mathfrak{f} = \mathfrak{p}_1^{n_1}\mathfrak{p}_2^{n_2}$, and $\omega(\mathfrak{f}\mathfrak{p}_1^{-n_1}\mathfrak{p}_2^{-n_2}) = \omega_K$ in this case. Using this fact, one can check that if assumption (4.10) holds, then

$$\biggl(\sum_{i=1}^{2} \frac{\omega(\mathfrak{f}\mathfrak{p}_i^{-n_i})}{\phi(\mathfrak{p}_i^{n_i})} - \frac{\omega(\mathfrak{f}\mathfrak{p}_1^{-n_1}\mathfrak{p}_2^{-n_2})}{\phi(\mathfrak{p}_1^{n_1})\phi(\mathfrak{p}_2^{n_2})}\biggr) \leqslant \frac{1}{2}, \tag{4.13}$$

which yields $M_2 \leqslant \frac{1}{2}[K_{\mathfrak{f}} : K] - 1$. Thus, for any $\boldsymbol{N}_{\mathfrak{f}} \geqslant 1$ we have $M_1 > M_2$, and so the claim is proved. Furthermore, the proof of proposition 4.3 shows that there is a character ψ'' of $\mathrm{Cl}(\mathfrak{f})$ for which $\chi\psi''|_{\mathrm{Cl}(K_{\mathfrak{f}}/F)} \neq 1$, $\mathfrak{f}_\chi | \mathfrak{f}_{\chi\psi''}$ and $\mathfrak{p}_i | \mathfrak{f}_{\chi\psi''}$ for all i. So, by replacing χ by $\chi\psi''$, we get a character χ of $\mathrm{Cl}(\mathfrak{f})$ satisfying $\chi|_{\mathrm{Cl}(K_{\mathfrak{f}}/F)} \neq 1$ and $\mathfrak{p}_i | \mathfrak{f}_\chi$ for all i.

Since χ is non-trivial and $\mathfrak{f}_\chi \neq \mathcal{O}_K$, we have $S_{\mathfrak{f}}(\bar{\chi}, g_{\mathfrak{f}}) \neq 0$ by proposition 3.6. On the other hand, we deduce that

$$\begin{aligned} S_{\mathfrak{f}}(\bar{\chi}, g_{\mathfrak{f}}) &= \frac{1}{n} \sum_{C \in \mathrm{Cl}(\mathfrak{f})} \bar{\chi}(C) \log |g_{\mathfrak{f}}(C)^n| \\ &= \frac{1}{n} \sum_{C \in \mathrm{Cl}(\mathfrak{f})} \bar{\chi}(C) \log |(g_{\mathfrak{f}}(C_0)^n)^{\sigma(C)}| \quad (\text{by proposition 3.3}) \end{aligned}$$

$$= \frac{1}{n} \sum_{[C_1]\in \mathrm{Cl}(\mathfrak{f})/\mathrm{Cl}(K_\mathfrak{f}/F)} \left(\sum_{C_2 \in \mathrm{Cl}(K_\mathfrak{f}/F)} \bar{\chi}(C_1C_2) \log |(g_\mathfrak{f}(C_0)^n)^{\sigma(C_1C_2)}| \right)$$
$$= \frac{1}{n} \sum_{[C_1]\in \mathrm{Cl}(\mathfrak{f})/\mathrm{Cl}(K_\mathfrak{f}/F)} \bar{\chi}(C_1) \log |(g_\mathfrak{f}(C_0)^n)^{\sigma(C_1)}| \left(\sum_{C_2 \in \mathrm{Cl}(K_\mathfrak{f}/F)} \bar{\chi}(C_2) \right)$$
$$= 0,$$

because $g_\mathfrak{f}(C_0)^n \in F$ and $\chi|_{\mathrm{Cl}(K_\mathfrak{f}/F)} \neq 1$. This gives a contradiction. Therefore, $F = K_\mathfrak{f}$, and so $K_\mathfrak{f} = K(g_\mathfrak{f}(C)^n)$ for any $C \in \mathrm{Cl}(\mathfrak{f})$ since $g_\mathfrak{f}(C)^n = (g_\mathfrak{f}(C_0)^n)^{\sigma(C)}$ by proposition 3.3. □

Remark 4.7.

(i) If $\boldsymbol{N}_\mathfrak{f} = 2$ and $\mathfrak{f} = \mathfrak{p}_1^{n_1}\mathfrak{p}_2^{n_2}$, then one can show that the inequality (4.13) holds except in the case where $K \neq \mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-3})$, 2 is ramified in K and $\mathfrak{f} = \mathfrak{p}_{(2)}^2\mathfrak{p}_{(5)}$. Here, $\mathfrak{p}_{(p)}$ stands for a prime ideal of K lying over a prime number p. Therefore, we are able to establish theorem 4.6, again under the above condition.

(ii) Schertz conjectured [12, conjecture 6.8.3] that (4.11) holds for any non-trivial proper integral ideal $\mathfrak{f}$ of K. In theorem 4.6 we present a conditional proof of his conjecture.

5. Ray-class fields constructed by smaller generators

In this section we shall construct ray-class invariants over imaginary quadratic fields whose minimal polynomials have relatively small coefficients.

Let $K = \mathbb{Q}(\sqrt{-d})$ be an imaginary quadratic field with a square-free integer $d > 0$, let $\mathfrak{f}$ be a non-trivial proper integral ideal of K and let θ be as in (2.3). In what follows we adopt the notation of § 4.

Lemma 5.1. *Let $\boldsymbol{r}, \boldsymbol{s} \in (1/N)\mathbb{Z}^2 \setminus \mathbb{Z}^2$ for a positive integer $N \geqslant 2$. Then we obtain that*

$$\frac{g_{\boldsymbol{r}}(\theta)^{\gcd(2,N)\cdot N}}{g_{\boldsymbol{s}}(\theta)^{\gcd(2,N)\cdot N}}$$

lies in the ray-class field $K_{(N)} = K_\mathfrak{f}$ with $\mathfrak{f} = N\mathcal{O}_K$.

Proof. This is immediate from propositions 2.1 and 3.1. □

Lemma 5.2. *Let*

$$\mathfrak{f} = N\mathcal{O}_K = \prod_{i=1}^{r} \mathfrak{p}_i^{n_i}$$

for an integer $N \geqslant 2$ and let p be an odd prime dividing N (if any). Assume that $K_\mathfrak{f} \neq K_{\mathfrak{f}\mathfrak{p}_i^{-n_i}}$ for every i. Then there is an element $\beta \in \mathcal{O}_K$ prime to $6N$ for which

$N_{K/\mathbb{Q}}(\beta) \equiv 1 \pmod{\omega_{K_\mathfrak{f}}}$, and the ray class $[(\beta)] \in \mathrm{Cl}(\mathfrak{f})$ is of order k_p, where

$$k_p = \begin{cases} \dfrac{1}{\omega_K}\left(p - \left(\dfrac{d_K}{p}\right)\right) & \text{if } p \nmid d_K,\ \mathrm{ord}_p(N) = 1 \text{ and } N = p,\\ \dfrac{1}{2}\left(p - \left(\dfrac{d_K}{p}\right)\right) & \text{if } p \nmid d_K,\ \mathrm{ord}_p(N) = 1 \text{ and } N \neq p,\\ p & \text{otherwise.} \end{cases}$$

Here (d_K/p) is the Kronecker symbol.

Proof. Let

$$N' = \begin{cases} 4N & \text{if } 3|N,\\ 12N & \text{if } 3 \nmid N, \end{cases}$$

with prime decomposition $N' = \prod_\ell \ell^{n_\ell}$. Then $n_p = \mathrm{ord}_p(N') = \mathrm{ord}_p(N)$ and $\omega_{K_\mathfrak{f}}$ divides N' [6, ch. 9, lemma 4.3]. Hence, it suffices to find $\beta \in \mathcal{O}_K$ for which $N_{K/\mathbb{Q}}(\beta) \equiv 1 \pmod{N'}$ and the order of the ray class $[(\beta)] \in \mathrm{Cl}(\mathfrak{f})$ is k_p. For simplicity, we let $m = p - (d_K/p)$ and define a homomorphism

$$\begin{aligned} \tilde{N}_{K/\mathbb{Q},n} \colon (\mathcal{O}_K/n\mathcal{O}_K)^\times &\to (\mathbb{Z}/n\mathbb{Z})^\times \\ \omega + n\mathcal{O}_K &\mapsto N_{K/\mathbb{Q}}(\omega) + n\mathbb{Z} \end{aligned}$$

for each integer $n \geqslant 2$.

Case 1. First, suppose that $p \nmid d_K$ and $\mathrm{ord}_p(N) = 1$. We claim that the homomorphism

$$\tilde{N}_{K/\mathbb{Q},p} \colon (\mathcal{O}_K/p\mathcal{O}_K)^\times \to (\mathbb{Z}/p\mathbb{Z})^\times$$

is surjective and $\ker(\tilde{N}_{K/\mathbb{Q},p}) \cong \mathbb{Z}/m\mathbb{Z}$. Indeed, we can write

$$\mathcal{O}_K/p\mathcal{O}_K = \{x + y\sqrt{-d} + p\mathcal{O}_K \mid x, y \in \mathbb{F}_p\}$$

because $\gcd(2, p) = 1$. Then one can readily show that the map

$$\begin{aligned} \{\omega + p\mathcal{O}_K \in (\mathcal{O}_K/p\mathcal{O}_K)^\times \mid N_{K/\mathbb{Q}}(\omega) \equiv 1 \pmod{p}\} &\to \mathcal{C}(\mathbb{F}_p) \\ x + y\sqrt{-d} + p\mathcal{O}_K &\mapsto (x, y) \end{aligned}$$

is a well-defined isomorphism, where $\mathcal{C}\colon x^2 - (-d)y^2 = 1$ is the Pell conic over $\mathbb{F}_p$. Hence, $\ker(\tilde{N}_{K/\mathbb{Q},p}) \cong \mathcal{C}(\mathbb{F}_p) \cong \mathbb{Z}/m\mathbb{Z}$ [9, § 2.1] and the claim is proved by (4.1). We choose $\omega \in \mathcal{O}_K$ so that $\ker(\tilde{N}_{K/\mathbb{Q},p}) = \langle \omega + p\mathcal{O}_K \rangle$. Then, by the Chinese remainder theorem, there exist $\omega' \in \mathcal{O}_K$ for which for each prime ℓ divides N':

$$\omega' \equiv \begin{cases} \omega \pmod{\ell^{n_\ell}\mathcal{O}_K} & \text{if } \ell = p,\\ 1 \pmod{\ell^{n_\ell}\mathcal{O}_K} & \text{if } \ell \neq p. \end{cases}$$

We observe that ω' is prime to $6N$ and that $\omega' + N'\mathcal{O}_K$ is contained in $\ker(\tilde{N}_{K/\mathbb{Q},N'})$ and is of order m in $(\mathcal{O}_K/N\mathcal{O}_K)^\times$. If $N = p$, then the ray class $[(\omega')] \in \mathrm{Cl}(\mathfrak{f})$ is of order m/ω_K because

$$\{\varepsilon + p\mathcal{O}_K \in (\mathcal{O}_K/p\mathcal{O}_K)^\times \mid \varepsilon \in \mathcal{O}_K^\times\} \subset \ker(\tilde{N}_{K/\mathbb{Q},p}) = \langle \omega' + p\mathcal{O}_K \rangle.$$

https://doi.org/10.1017/S0308210516000263 Published online by Cambridge University Press

When $N \neq p$, we derive that

$$(\text{the order of } [(\omega')] \text{ in } \mathrm{Cl}(\mathfrak{f})) = \begin{cases} m/2 & \text{if } -1 + N\mathcal{O}_K \in \langle \omega' + N\mathcal{O}_K \rangle, \\ m & \text{otherwise.} \end{cases}$$

Therefore, we can find $\beta \in \mathcal{O}_K$ with the desired properties.

Case 2. Now, assume that $\mathrm{ord}_p(N) > 1$ or $p | d_K$. Let

$$\beta = \begin{cases} 1 + \dfrac{2N}{p}\sqrt{-d} & \text{if } p = 3, \\ 1 + \dfrac{6N}{p}\sqrt{-d} & \text{if } p \neq 3. \end{cases} \tag{5.1}$$

Then $N_{K/\mathbb{Q}}(\beta) \equiv 1 \pmod{N'}$ and $\beta + N\mathcal{O}_K$ is of order p in $(\mathcal{O}_K/N\mathcal{O}_K)^\times$ because p^2 divides Nd. And we claim that

$$\{\varepsilon + N\mathcal{O}_K \in (\mathcal{O}_K/N\mathcal{O}_K)^\times \mid \varepsilon \in \mathcal{O}_K^\times\} \cap \langle \beta + N\mathcal{O}_K \rangle = \{1 + N\mathcal{O}_K\},$$

since p is an odd prime and $K_\mathfrak{f} \neq K_{\mathfrak{f}\mathfrak{p}_i^{-n_i}}$ for every i. Thus, the ray class $[(\beta)] \in \mathrm{Cl}(\mathfrak{f})$ is of order p, as desired. □

Remark 5.3. If p is an odd prime such that $p - (d_K/p)$ is a power of 2, then p is either a Mersenne prime or a Fermat prime. Observe that forty-eight Mersenne primes and five Fermat primes were known as of May 2014.

Theorem 5.4. *Let $\mathfrak{f} = \prod_{i=1}^r \mathfrak{p}_i^{n_i}$ be a non-trivial proper integral ideal of K and let C' be an element of $\boldsymbol{G}\,(\subset \mathrm{Cl}(\mathfrak{f}))$ whose order is an odd prime p. Assume that $K_\mathfrak{f} \neq K_{\mathfrak{f}\mathfrak{p}_i^{-n_i}}$ and $|\boldsymbol{G}_i| > 2$ for every i. If $p > 3$ or $|\boldsymbol{G}_i| > 3$ for every i, then for any non-zero integer n the unit*

$$\frac{g_\mathfrak{f}(C')^n}{g_\mathfrak{f}(C_0)^n}$$

generates $K_\mathfrak{f}$ over K.

Moreover, if $\mathfrak{f} = N\mathcal{O}_K$ for an integer $N \geqslant 2$ and $C' = [(\beta')]$ for some $\beta' \in \mathcal{O}_K$ prime to $6N$ with $N_{K/\mathbb{Q}}(\beta') \equiv 1 \pmod{\omega_{K_\mathfrak{f}}}$, then

$$K_\mathfrak{f} = K\left(\frac{g_{\left[\begin{smallmatrix} s/N \\ t/N \end{smallmatrix}\right]}(\theta)^m}{g_{\left[\begin{smallmatrix} 0 \\ 1/N \end{smallmatrix}\right]}(\theta)^m}\right),$$

where $\beta' = s\theta + t$ with $s, t \in \mathbb{Z}$ and

$$m = \begin{cases} \gcd(N, 3) & \text{if } N \text{ is odd,} \\ 4 \cdot \gcd(\frac{1}{2}N, 3) & \text{if } N \text{ is even.} \end{cases}$$

Proof. Let $F = K(g_\mathfrak{f}(C')^n / g_\mathfrak{f}(C_0)^n)$. Suppose $F \subsetneq K_\mathfrak{f}$, namely, $\mathrm{Cl}(K_\mathfrak{f}/F) \neq \{1\}$. We then claim that there exists a character χ of $\mathrm{Cl}(\mathfrak{f})$ such that $\chi|_{\mathrm{Cl}(K_\mathfrak{f}/F)} \neq 1$, $\chi(C') \neq 1$ and $\mathfrak{p}_i | \mathfrak{f}_\chi$ for every i. Indeed, one can achieve

$$|\{\text{characters } \chi \neq 1 \text{ of } \mathrm{Cl}(\mathfrak{f}) \mid \chi(C') = 1\}| = \frac{1}{p}[K_\mathfrak{f} : K] - 1.$$

It also follows from (4.12) that

$$|\{\text{characters } \chi \text{ of } \mathrm{Cl}(\mathfrak{f}) \mid \chi|_{\mathrm{Cl}(K_\mathfrak{f}/F)} \neq 1\}| \geqslant \tfrac{1}{2}[K_\mathfrak{f}:K] > \frac{1}{p}[K_\mathfrak{f}:K] - 1.$$

Thus, there is a character χ of $\mathrm{Cl}(\mathfrak{f})$ satisfying $\chi|_{\mathrm{Cl}(K_\mathfrak{f}/F)} \neq 1$ and $\chi(C') \neq 1$. Since $C' \in \boldsymbol{G}$, we may write $C' = [(\beta')]$ for some $\beta' \in \mathcal{O}_K$ which is prime to $\mathfrak{f}$. Choose $C'' \in \mathrm{Cl}(K_\mathfrak{f}/F)$ of prime order ℓ satisfying $\chi(C'') \neq 1$. Here, we assume that $\mathfrak{f}_\chi$ is not divided by $\mathfrak{p}_i$ for some i. We then consider the following two cases.

Case 1 ($C'' \notin \boldsymbol{G}$). The proof of proposition 4.3 shows that there exists a non-trivial character ψ of $\boldsymbol{G}_i$ such that $\psi([\beta' + \mathfrak{p}_i^{n_i}]) \neq \chi(C')^{-1}$. And, we can extend ψ to a character ψ' of $\boldsymbol{G}$ whose conductor is divisible only by $\mathfrak{p}_i$. Since $C'' \notin \boldsymbol{G}$ and $\psi'((C'')^\ell) = 1$, one can also extend ψ' to a character ψ'' of $\mathrm{Cl}(\mathfrak{f})$ so as to have $\psi''(C'') = 1$ by lemma 4.2. Note that the character $\chi\psi''$ of $\mathrm{Cl}(\mathfrak{f})$ satisfies $\chi\psi''(C') \neq 1$, $\chi\psi''(C'') = \chi(C'') \neq 1$, $\mathfrak{p}_i|\mathfrak{f}_{\chi\psi''}$ and $\mathfrak{f}_\chi|\mathfrak{f}_{\chi\psi''}$. And we replace χ by $\chi\psi''$.

Case 2 ($C'' \in \boldsymbol{G}$). Let $\beta'' \in \mathcal{O}_K$ such that $C'' = [(\beta'')]$ in $\mathrm{Cl}(\mathfrak{f})$.

(i) If $\boldsymbol{G}_i \neq \langle[\beta'' + \mathfrak{p}_i^{n_i}]\rangle$, we can choose a trivial character ψ_1 of the proper subgroup $\langle[\beta'' + \mathfrak{p}_i^{n_i}]\rangle$ of $\boldsymbol{G}_i$. Since $\langle[\beta'' + \mathfrak{p}_i^{n_i}]\rangle \cong \{1\}$ or $\mathbb{Z}/\ell\mathbb{Z}$ in the group $\boldsymbol{G}_i$, we have either $\langle[\beta' + \mathfrak{p}_i^{n_i}]\rangle = \langle[\beta'' + \mathfrak{p}_i^{n_i}]\rangle \subsetneq \boldsymbol{G}_i$ or $\langle[\beta' + \mathfrak{p}_i^{n_i}]\rangle \cap \langle[\beta'' + \mathfrak{p}_i^{n_i}]\rangle = \{1\}$. And, by using lemma 4.2, we can extend ψ_1 to a non-trivial character ψ of $\boldsymbol{G}_i$ such that $\psi(\beta' + \mathfrak{p}_i^{n_i}) \neq \chi(C')^{-1}$ due to the fact that $p \geqslant 3$.

(ii) Now assume that $\boldsymbol{G}_i = \langle[\beta'' + \mathfrak{p}_i^{n_i}]\rangle \cong \mathbb{Z}/\ell\mathbb{Z}$. Then $\ell > 2$ because $|\boldsymbol{G}_i| > 2$. If $\beta' + \mathfrak{p}_i^{n_i} \in \{\alpha + \mathfrak{p}_i^{n_i} \in (\mathcal{O}_K/\mathfrak{p}_i^{n_i})^\times \mid \alpha \in \mathcal{O}_K^\times\}$, there is a non-trivial character ψ of $\boldsymbol{G}_i$ for which $\psi([\beta'' + \mathfrak{p}_i^{n_i}]) \neq \chi(C'')^{-1}$. Observe that $\psi([\beta' + \mathfrak{p}_i^{n_i}]) = 1$. On the other hand, if $\beta' + \mathfrak{p}_i^{n_i} \notin \{\alpha + \mathfrak{p}_i^{n_i} \in (\mathcal{O}_K/\mathfrak{p}_i^{n_i})^\times \mid \alpha \in \mathcal{O}_K^\times\}$, then $\langle[\beta' + \mathfrak{p}_i^{n_i}]\rangle = \langle[\beta'' + \mathfrak{p}_i^{n_i}]\rangle$ and $p = \ell$. And we see that $p, \ell > 3$ by hypothesis. Let ψ_1 be a character of $\boldsymbol{G}_i$ such that $\psi_1([\beta' + \mathfrak{p}_i^{n_i}]) = \zeta_p$. Then $\psi, \psi^2, \ldots, \psi^{p-1}$ are distinct non-trivial characters of $\boldsymbol{G}_i$ and we derive

$$|\{\psi_1^j \mid \psi_1^j([\beta' + \mathfrak{p}_i^{n_i}]) \neq \chi(C')^{-1}\}_{1 \leqslant j \leqslant p-1}| = p - 2.$$

Meanwhile, $\psi_1([\beta'' + \mathfrak{p}_i^{n_i}]) = \zeta_p^s$ for some $1 \leqslant s \leqslant p-1$. If

$$\psi_1^{j_1}([\beta'' + \mathfrak{p}_i^{n_i}]) = \psi_1^{j_2}([\beta'' + \mathfrak{p}_i^{n_i}])$$

for some $1 \leqslant j_1, j_2 \leqslant p-1$, then $\zeta_p^{s(j_1 - j_2)} = 1$, and so $j_1 = j_2$. Hence, we have

$$|\{\psi_1^j \mid \psi_1^j([\beta' + \mathfrak{p}_i^{n_i}]) \neq \chi(C')^{-1},\ \psi_1^j([\beta'' + \mathfrak{p}_i^{n_i}]) \neq \chi(C'')^{-1}\}_{1 \leqslant j \leqslant p-1}| \geqslant p - 3 > 0.$$

We choose a character ψ of $\boldsymbol{G}_i$ in the above set.

Therefore, in all cases we can extend ψ to a character ψ'' of $\mathrm{Cl}(\mathfrak{f})$ in a similar fashion, and it satisfies $\chi\psi''(C') \neq 1$, $\chi\psi''(C'') \neq 1$, $\mathfrak{p}_i|\mathfrak{f}_{\chi\psi''}$ and $\mathfrak{f}_\chi|\mathfrak{f}_{\chi\psi''}$. Now, we replace χ by $\chi\psi''$.

By continuing this process for every i, we get the claim.

Since χ is non-trivial and $\mathfrak{p}_i|\mathfrak{f}_\chi$ for every i, we have $S_\mathfrak{f}(\bar{\chi}, g_\mathfrak{f}) \neq 0$ by proposition 3.6 and remark 3.7. On the other hand, we deduce that

$$\begin{aligned}
&(\chi(C') - 1)S_\mathfrak{f}(\bar{\chi}, g_\mathfrak{f})\\
&\quad = (\bar{\chi}(C'^{-1}) - 1) \sum_{C\in \mathrm{Cl}(\mathfrak{f})} \bar{\chi}(C) \log|g_\mathfrak{f}(C)|\\
&\quad = \frac{1}{n} \sum_{C\in \mathrm{Cl}(\mathfrak{f})} \bar{\chi}(C) \log\left|\frac{g_\mathfrak{f}(CC')^n}{g_\mathfrak{f}(C)^n}\right|\\
&\quad = \frac{1}{n} \sum_{C\in \mathrm{Cl}(\mathfrak{f})} \bar{\chi}(C) \log\left|\left(\frac{g_\mathfrak{f}(C')^n}{g_\mathfrak{f}(C_0)^n}\right)^{\sigma(C)}\right| \quad \text{(by proposition 3.3)}\\
&\quad = \frac{1}{n} \sum_{[C_1]\in \mathrm{Cl}(\mathfrak{f})/\mathrm{Cl}(K_\mathfrak{f}/F)} \left(\sum_{C_2\in \mathrm{Cl}(K_\mathfrak{f}/F)} \bar{\chi}(C_1C_2) \log\left|\left(\frac{g_\mathfrak{f}(C')^n}{g_\mathfrak{f}(C_0)^n}\right)^{\sigma(C_1C_2)}\right|\right)\\
&\quad = \frac{1}{n} \sum_{[C_1]\in \mathrm{Cl}(\mathfrak{f})/\mathrm{Cl}(K_\mathfrak{f}/F)} \bar{\chi}(C_1) \log\left|\left(\frac{g_\mathfrak{f}(C')^n}{g_\mathfrak{f}(C_0)^n}\right)^{\sigma(C_1)}\right|\left(\sum_{C_2\in \mathrm{Cl}(K_\mathfrak{f}/F)} \bar{\chi}(C_2)\right)\\
&\quad = 0,
\end{aligned}$$

because $\bar{\chi}$ is non-trivial on $\mathrm{Cl}(K_\mathfrak{f}/F)$. And it yields a contradiction, since $\chi(C')-1 \neq 0$. Therefore, we conclude that $F = K_\mathfrak{f}$.

If $\mathfrak{f} = N\mathcal{O}_K$ for a positive integer $N \geqslant 2$ and $\beta' = s\theta + t$ is prime to $6N$ with $N_{K/\mathbb{Q}}(\beta') \equiv 1 \pmod{\omega_{K_\mathfrak{f}}}$, then any Nth root of the value $g_\mathfrak{f}(C')/g_\mathfrak{f}(C_0)$ generates $K_\mathfrak{f}$ over K by lemma 3.5. Write $\min(\theta, \mathbb{Q}) = X^2 + B_\theta X + C_\theta$. Then we have, by definition,

$$g_\mathfrak{f}(C_0) = g_{\left[\begin{smallmatrix}0\\1/N\end{smallmatrix}\right]}(\theta)^{12N}$$

and

$$g_\mathfrak{f}(C') = g_\mathfrak{f}(C_0)^{\sigma(C')} = g_{\left[\begin{smallmatrix}t-B_\theta s & s\\ -C_\theta s & t\end{smallmatrix}\right]\left[\begin{smallmatrix}0\\1/N\end{smallmatrix}\right]}(\theta)^{12N} = g_{\left[\begin{smallmatrix}s/N\\t/N\end{smallmatrix}\right]}(\theta)^{12N}$$

by propositions 2.3, 3.2 and 3.3. Therefore,

$$K_\mathfrak{f} = K\left(\frac{g_{\left[\begin{smallmatrix}s/N\\t/N\end{smallmatrix}\right]}(\theta)^{12}}{g_{\left[\begin{smallmatrix}0\\1/N\end{smallmatrix}\right]}(\theta)^{12}}\right),$$

and hence we get the conclusion by lemma 5.1. □

Remark 5.5.

(i) As in lemma 4.4 one can show that $|\boldsymbol{G}_i| = 3$ if and only if $\mathfrak{p}_i^{n_i}$ satisfies one of the following conditions.

Case 1 ($K \neq \mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-3})$).

- 2 is inert in K, $\mathfrak{p}_i$ is lying over 2 and $n_i = 1$.
- 3 is not inert in K, $\mathfrak{p}_i$ is lying over 3 and $n_i = 2$.
- 7 is not inert in K, $\mathfrak{p}_i$ is lying over 7 and $n_i = 1$.

CASE 2 ($K = \mathbb{Q}(\sqrt{-1})$).

- $\mathfrak{p}_i$ is lying over 13 and $n_i = 1$.

CASE 3 ($K = \mathbb{Q}(\sqrt{-3})$).

- $\mathfrak{p}_i$ is lying over 3 and $n_i = 3$.
- $\mathfrak{p}_i$ is lying over 19 and $n_i = 1$.

The first claim of theorem 5.4 would be an improvement of Schertz's result [12, theorem 6.8.4].

REMARK 5.6.

(i) Suppose

$$\left(\frac{g_{\mathfrak{f}}(C')}{g_{\mathfrak{f}}(C_0)}\right)^{\sigma(C)} \neq \frac{g_{\mathfrak{f}}(C')}{g_{\mathfrak{f}}(C_0)}$$

for every $C \in \boldsymbol{G} \setminus \{1\}$. Then we may consider only case 1 in the proof of theorem 5.4. Thus, one can prove that theorem 5.4 is still valid for any prime p with the assumptions $K_{\mathfrak{f}} \neq K_{\mathfrak{f}\mathfrak{p}_i^{-n_i}}$ and $|\boldsymbol{G}_i| > 2$ for every i.

(ii) Let $\mathfrak{f} = N\mathcal{O}_K$ for a positive integer $N \geqslant 2$ and let ℓ be an odd prime dividing N. For any odd prime p dividing k_ℓ, there exists $\beta' \in \mathcal{O}_K$ prime to $6N$ for which $N_{K/\mathbb{Q}}(\beta') \equiv 1 \pmod{\omega_{K_{\mathfrak{f}}}}$ and the order of the ray class $[(\beta')]$ is p by lemma 5.2.

The following corollary would be an explicit example of theorem 5.4.

COROLLARY 5.7. *Let $\mathfrak{f} = N\mathcal{O}_K$ for a positive integer $N \geqslant 2$ and let p be an odd prime dividing N (if any). Further, we set $\beta \in \mathcal{O}_K$ as in (5.1) and $C' = [(\beta)] \in \mathrm{Cl}(\mathfrak{f})$. Assume that $K_{\mathfrak{f}} \neq K_{\mathfrak{f}\mathfrak{p}_i^{-n_i}}$, $|\boldsymbol{G}_i| > 2$ for every i and p^2 divides Nd_K.*

(i) *If $p = 3$ and $|\boldsymbol{G}_i| > 3$ for every i, then the special value*

$$\gamma = \begin{cases} \dfrac{g_{\left[\begin{smallmatrix} 2/3 \\ 1/N \end{smallmatrix}\right]}(\theta)^3}{g_{\left[\begin{smallmatrix} 0 \\ 1/N \end{smallmatrix}\right]}(\theta)^3} & \text{if } d_K \equiv 0 \pmod 4, \\[2ex] \dfrac{g_{\left[\begin{smallmatrix} 4/3 \\ 2/3+1/N \end{smallmatrix}\right]}(\theta)^3}{g_{\left[\begin{smallmatrix} 0 \\ 1/N \end{smallmatrix}\right]}(\theta)^3} & \text{if } d_K \equiv 1 \pmod 4, \end{cases}$$

generates $K_{\mathfrak{f}}$ $(= K_{(N)})$ over K. It is a unit in $K_{\mathfrak{f}}$ and is a $4N$th root of $g_{\mathfrak{f}}(C')/g_{\mathfrak{f}}(C_0)$.

(ii) *If $p>3$, then the special value*

$$\gamma=\begin{cases}\dfrac{g_{\left[\begin{smallmatrix}6/p\\1/N\end{smallmatrix}\right]}(\theta)}{g_{\left[\begin{smallmatrix}0\\1/N\end{smallmatrix}\right]}(\theta)} & \text{if } d_K\equiv 0 \pmod 4,\\[2ex] \dfrac{g_{\left[\begin{smallmatrix}12/p\\6/p+1/N\end{smallmatrix}\right]}(\theta)}{g_{\left[\begin{smallmatrix}0\\1/N\end{smallmatrix}\right]}(\theta)} & \text{if } d_K\equiv 1 \pmod 4,\end{cases}$$

generates $K_{\mathfrak{f}}$ over K. Further, it is a unit in $K_{\mathfrak{f}}$ and is a $12N$th root of $g_{\mathfrak{f}}(C')/g_{\mathfrak{f}}(C_0)$.

Proof. Note that β is prime to $6N$, $N_{K/\mathbb{Q}}(\beta)\equiv 1 \pmod{\omega_{K_{\mathfrak{f}}}}$ and the ray class $[(\beta)]\in \mathrm{Cl}(\mathfrak{f})$ is of order p by lemma 5.2. Hence, if $p>3$ or $|\boldsymbol{G}_i|>3$ for every i, then by theorem 5.4, we obtain

$$K_{\mathfrak{f}}=K\left(\frac{g_{\mathfrak{f}}(C')}{g_{\mathfrak{f}}(C_0)}\right).$$

(i) If $p=3$, then we can write

$$\beta=\begin{cases}\dfrac{2N}{3}\theta+1 & \text{if } d_K\equiv 0 \pmod 4,\\[1ex] \dfrac{4N}{3}\theta+\dfrac{2N}{3}+1 & \text{if } d_K\equiv 1 \pmod 4.\end{cases}$$

Here we observe that

$$g_{\mathfrak{f}}(C_0)=g_{\left[\begin{smallmatrix}0\\1/N\end{smallmatrix}\right]}(\theta)^{12N}$$

by definition and

$$g_{\mathfrak{f}}(C')=g_{\mathfrak{f}}(C_0)^{\sigma(C')}=\begin{cases}g_{\left[\begin{smallmatrix}2/3\\1/N\end{smallmatrix}\right]}(\theta)^{12N} & \text{if } d_K\equiv 0 \pmod 4,\\ g_{\left[\begin{smallmatrix}4/3\\2/3+1/N\end{smallmatrix}\right]}(\theta)^{12N} & \text{if } d_K\equiv 1 \pmod 4,\end{cases}$$

by propositions 2.3, 3.2 and 3.3. Since $\zeta_N\in\mathcal{F}_N$, we see that the functions

$$\frac{g_{\left[\begin{smallmatrix}2/3\\1/N\end{smallmatrix}\right]}(\tau)^3}{g_{\left[\begin{smallmatrix}0\\1/N\end{smallmatrix}\right]}(\tau)^3} \quad\text{and}\quad \frac{g_{\left[\begin{smallmatrix}4/3\\2/3+1/N\end{smallmatrix}\right]}(\tau)^3}{g_{\left[\begin{smallmatrix}0\\1/N\end{smallmatrix}\right]}(\tau)^3}$$

belong to $\mathcal{F}_N$ by proposition 3.1. Thus, its special value at θ lies in $K_{\mathfrak{f}}=K_{(N)}$ by proposition 2.1, and so it generates $K_{\mathfrak{f}}$ over K.

(ii) If $p>3$, then we may write

$$\beta=\begin{cases}\dfrac{6N}{p}\theta+1 & \text{if } d_K\equiv 0 \pmod 4,\\[1ex] \dfrac{12N}{p}\theta+\dfrac{6N}{p}+1 & \text{if } d_K\equiv 1 \pmod 4.\end{cases}$$

https://doi.org/10.1017/S0308210516000263 Published online by Cambridge University Press

And, in a similar way one can readily show that the special value γ^p generates $K_{\mathfrak{f}}$ over K. On the other hand, γ^{12} is an element of $K_{\mathfrak{f}}$ by theorem 5.4. Therefore, we get

$$K_{\mathfrak{f}} = K(\gamma),$$

owing to the fact that $\gcd(p, 12) = 1$.

□

Example 5.8. Let $K = \mathbb{Q}(\sqrt{-7})$ and $\theta = \frac{1}{2}(-1 + \sqrt{-7})$. Then the class number h_K is 1.

(i) Let $\mathfrak{f} = 9\mathcal{O}_K$. Then 3 is inert in K and so $|\boldsymbol{G}_i| > 3$ for every i. Hence, the special value

$$\gamma = \frac{g_{\left[\begin{smallmatrix} 4/3 \\ 7/9 \end{smallmatrix}\right]}(\theta)^3}{g_{\left[\begin{smallmatrix} 0 \\ 1/9 \end{smallmatrix}\right]}(\theta)^3}$$

generates $K_{(9)}$ over K by corollary 5.7.

Here we note that $\mathrm{Gal}(K_{(9)}/K) \cong W_{9,\theta}/\{\pm I_2\}$ by proposition 2.4, and hence we obtain

$$\begin{aligned} &W_{9,\theta}/\{\pm I_2\} \\ &= \left\{ \begin{bmatrix}1&0\\0&1\end{bmatrix}, \begin{bmatrix}2&0\\0&2\end{bmatrix}, \begin{bmatrix}4&0\\0&4\end{bmatrix}, \begin{bmatrix}8&7\\1&0\end{bmatrix}, \begin{bmatrix}0&7\\1&1\end{bmatrix}, \begin{bmatrix}1&7\\1&2\end{bmatrix}, \begin{bmatrix}2&7\\1&3\end{bmatrix}, \begin{bmatrix}3&7\\1&4\end{bmatrix}, \right. \\ &\quad \begin{bmatrix}4&7\\1&5\end{bmatrix}, \begin{bmatrix}5&7\\1&6\end{bmatrix}, \begin{bmatrix}6&7\\1&7\end{bmatrix}, \begin{bmatrix}7&7\\1&8\end{bmatrix}, \begin{bmatrix}7&5\\2&0\end{bmatrix}, \begin{bmatrix}8&5\\2&1\end{bmatrix}, \begin{bmatrix}0&5\\2&2\end{bmatrix}, \begin{bmatrix}1&5\\2&3\end{bmatrix}, \\ &\quad \begin{bmatrix}2&5\\2&4\end{bmatrix}, \begin{bmatrix}3&5\\2&5\end{bmatrix}, \begin{bmatrix}4&5\\2&6\end{bmatrix}, \begin{bmatrix}5&5\\2&7\end{bmatrix}, \begin{bmatrix}6&5\\2&8\end{bmatrix}, \begin{bmatrix}7&3\\3&1\end{bmatrix}, \begin{bmatrix}8&3\\3&2\end{bmatrix}, \begin{bmatrix}1&3\\3&4\end{bmatrix}, \\ &\quad \begin{bmatrix}2&3\\3&5\end{bmatrix}, \begin{bmatrix}4&3\\3&7\end{bmatrix}, \begin{bmatrix}5&3\\3&8\end{bmatrix}, \begin{bmatrix}5&1\\4&0\end{bmatrix}, \begin{bmatrix}6&1\\4&1\end{bmatrix}, \begin{bmatrix}7&1\\4&2\end{bmatrix}, \begin{bmatrix}8&1\\4&3\end{bmatrix}, \begin{bmatrix}0&1\\4&4\end{bmatrix}, \\ &\quad \left. \begin{bmatrix}1&1\\4&5\end{bmatrix}, \begin{bmatrix}2&1\\4&6\end{bmatrix}, \begin{bmatrix}3&1\\4&7\end{bmatrix}, \begin{bmatrix}4&1\\4&8\end{bmatrix} \right\}. \end{aligned}$$

And, in general, if $\alpha \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I_2\}$ for a positive integer $N \geqslant 2$, then one can find $\alpha' \in \mathrm{SL}_2(\mathbb{Z})$ satisfying

$$\alpha \equiv \begin{bmatrix}1 & 0 \\ 0 & \det(\alpha)\end{bmatrix} \cdot \alpha' \pmod{N}$$

by (2.1). If a function $g_{\boldsymbol{r}}(\tau)^m / g_{\boldsymbol{s}}(\tau)^m$ lies in $\mathcal{F}_N$ for some $\boldsymbol{r}, \boldsymbol{s} \in \mathbb{Q}^2 \setminus \mathbb{Z}^2$ and $m \in \mathbb{Z}_{>0}$, we attain

$$\left(\frac{g_{\boldsymbol{r}}(\tau)^m}{g_{\boldsymbol{s}}(\tau)^m}\right)^{\alpha} = \frac{a(\boldsymbol{r})}{a(\boldsymbol{s})} \cdot \frac{g_{{}^t\alpha'\left[\begin{smallmatrix}1 & 0 \\ 0 & \det(\alpha)\end{smallmatrix}\right]\boldsymbol{r}}(\tau)^m}{g_{{}^t\alpha'\left[\begin{smallmatrix}1 & 0 \\ 0 & \det(\alpha)\end{smallmatrix}\right]\boldsymbol{s}}(\tau)^m}$$

by (2.2) and proposition 3.2. Here

$$a(\boldsymbol{r}) = \begin{cases} -1 & \text{if } mNr_2(r_1-1) \text{ is odd and } \det(\alpha) \text{ is even}, \\ 1 & \text{otherwise}, \end{cases}$$

for $\boldsymbol{r} = \left[\begin{smallmatrix} r_1 \\ r_2 \end{smallmatrix}\right] \in \mathbb{Q}^2 \setminus \mathbb{Z}^2$. In our case, the function

$$\frac{g_{\left[\begin{smallmatrix} 4/3 \\ 7/9 \end{smallmatrix}\right]}(\tau)^3}{g_{\left[\begin{smallmatrix} 0 \\ 1/9 \end{smallmatrix}\right]}(\tau)^3}$$

belongs to $\mathcal{F}_9$ and so we can find all conjugates of γ over K by using proposition 2.4. Therefore, we derive the minimal polynomial of γ over $\mathbb{Q}$ as

$$\begin{aligned} \min(\gamma, \mathbb{Q}) = \prod_{\tau \in \mathrm{Gal}(K_{(9)}/K)} (X - \gamma^\tau)(X - \overline{\gamma^\tau}) \\ = X^{72} + 90X^{71} + 1\,152X^{70} - 22\,371X^{69} + 458\,820X^{68} - 29\,836\,953X^{67} \\ + 491\,027\,613X^{66} - 1\,938\,660\,903X^{65} - 20\,725\,828\,920X^{64} \\ + 218\,606\,201\,947X^{63} - 87\,981\,391\,440X^{62} - 9\,726\,726\,330\,846X^{61} \\ + 74\,685\,511\,048\,146X^{60} - 296\,777\,453\,271\,966X^{59} \\ + 741\,369\,035\,579\,850X^{58} - 1\,250\,575\,046\,567\,529X^{57} \\ + 1\,668\,303\,706\,335\,570X^{56} - 3\,404\,755\,297\,594\,260X^{55} \\ + 12\,286\,071\,601\,634\,287X^{54} - 32\,591\,232\,085\,278\,402X^{53} \\ + 35\,114\,715\,622\,084\,023X^{52} + 37\,809\,379\,416\,794\,814X^{51} \\ - 111\,424\,993\,786\,127\,475X^{50} - 44\,163\,687\,277\,340\,892X^{49} \\ + 282\,536\,182\,740\,148\,884X^{48} - 43\,713\,385\,246\,904\,949X^{47} \\ - 422\,588\,747\,471\,994\,153X^{46} + 222\,731\,731\,243\,593\,448X^{45} \\ + 334\,105\,708\,870\,044\,999X^{44} - 414\,268\,957\,496\,144\,781X^{43} \\ + 13\,834\,474\,218\,095\,754X^{42} + 634\,423\,686\,065\,669\,232X^{41} \\ - 404\,320\,599\,974\,193\,246X^{40} - 761\,298\,152\,585\,541\,393X^{39} \\ + 489\,778\,367\,476\,257\,828X^{38} + 416\,185\,685\,059\,783\,914X^{37} \\ - 442\,068\,360\,347\,754\,785X^{36} + 416\,185\,685\,059\,783\,914X^{35} \\ + 489\,778\,367\,476\,257\,828X^{34} - 761\,298\,152\,585\,541\,393X^{33} \\ - 404\,320\,599\,974\,193\,246X^{32} + 634\,423\,686\,065\,669\,232X^{31} \\ + 13\,834\,474\,218\,095\,754X^{30} - 414\,268\,957\,496\,144\,781X^{29} \\ + 334\,105\,708\,870\,044\,999X^{28} + 222\,731\,731\,243\,593\,448X^{27} \\ - 422\,588\,747\,471\,994\,153X^{26} - 43\,713\,385\,246\,904\,949X^{25} \\ + 282\,536\,182\,740\,148\,884X^{24} - 44\,163\,687\,277\,340\,892X^{23} \\ - 111\,424\,993\,786\,127\,475X^{22} + 37\,809\,379\,416\,794\,814X^{21} \end{aligned}$$

https://doi.org/10.1017/S0308210516000263 Published online by Cambridge University Press

$$
\begin{aligned}
&+ 35\,114\,715\,622\,084\,023X^{20} - 32\,591\,232\,085\,278\,402X^{19}\\
&+ 12\,286\,071\,601\,634\,287X^{18} - 3\,404\,755\,297\,594\,260X^{17}\\
&+ 1\,668\,303\,706\,335\,570X^{16} - 1\,250\,575\,046\,567\,529X^{15}\\
&+ 741\,369\,035\,579\,850X^{14} - 296\,777\,453\,271\,966X^{13}\\
&+ 74\,685\,511\,048\,146X^{12} - 9\,726\,726\,330\,846X^{11}\\
&- 87\,981\,391\,440X^{10} + 218\,606\,201\,947X^{9} - 20\,725\,828\,920X^{8}\\
&- 1\,938\,660\,903X^{7} + 491\,027\,613X^{6} - 29\,836\,953X^{5} + 458\,820X^{4}\\
&- 22\,371X^{3} + 1\,152X^{2} + 90X + 1,
\end{aligned}
$$

which claims that γ is a unit as desired.

On the other hand, the Siegel–Ramachandra invariant

$$g_{\mathfrak{f}}(C_0) = g_{\left[\begin{smallmatrix}0\\1/9\end{smallmatrix}\right]}(\theta)^{108}$$

also generates $K_{(9)}$ over K by theorem 4.6. Observe that it is a real algebraic integer, and so its minimal polynomial over K has integer coefficients [6, lemma 2.1 and theorem 2.2]. One can then compute the minimal polynomial of $g_{\left[\begin{smallmatrix}0\\1/9\end{smallmatrix}\right]}(\theta)^{108}$ over K as follows:

$$
\begin{aligned}
&\min\left(g_{\left[\begin{smallmatrix}0\\1/9\end{smallmatrix}\right]}(\theta)^{108}, K\right)\\
&\quad\approx X^{36} - 5.8014\times10^{16}X^{35} + 1.2510\times10^{33}X^{34} - 1.2073\times10^{49}X^{33}\\
&\qquad + 5.2876\times10^{64}X^{32} - 1.3770\times10^{80}X^{31} + 4.5041\times10^{95}X^{30}\\
&\qquad + 7.1821\times10^{109}X^{29} + 3.5929\times10^{125}X^{28} + 6.0405\times10^{140}X^{27}\\
&\qquad - 2.6727\times10^{153}X^{26} + 4.0906\times10^{166}X^{25} + 1.5461\times10^{178}X^{24}\\
&\qquad + 2.5470\times10^{189}X^{23} - 8.8165\times10^{197}X^{22} + 1.2086\times10^{206}X^{21}\\
&\qquad - 6.5232\times10^{213}X^{20} + 1.1931\times10^{221}X^{19} + 1.1532\times10^{226}X^{18}\\
&\qquad + 1.8902\times10^{231}X^{17} + 5.0656\times10^{233}X^{16} + 4.0609\times10^{234}X^{15}\\
&\qquad + 1.3087\times10^{235}X^{14} + 1.8279\times10^{235}X^{13} + 1.0208\times10^{235}X^{12}\\
&\qquad + 1.3732\times10^{234}X^{11} - 5.1693\times10^{229}X^{10} + 1.5848\times10^{225}X^{9}\\
&\qquad + 1.2122\times10^{218}X^{8} - 1.7829\times10^{211}X^{7} + 1.2402\times10^{204}X^{6}\\
&\qquad + 5.8968\times10^{184}X^{5} + 7.7183\times10^{164}X^{4} + 1.3109\times10^{144}X^{3}\\
&\qquad - 1.2605\times10^{110}X^{2} + 1.1125\times10^{76}X + 5.8150\times10^{25}.
\end{aligned}
$$

But, we notice here that the coefficients of $\min(\gamma, \mathbb{Q})$ are much smaller than those of $\min(g_{\left[\begin{smallmatrix}0\\1/9\end{smallmatrix}\right]}(\theta)^{108}, K)$.

(ii) Let $\mathfrak{f} = 5\mathcal{O}_K$. Then 5 is inert in K and so $|\boldsymbol{G}_i| > 3$ for every i. By lemma 5.2 we get an element $\beta \in \mathcal{O}_K$ prime to 30 for which $N_{K/\mathbb{Q}}(\beta) \equiv 1 \pmod{\omega_{K_{\mathfrak{f}}}}$ and the ray class $[(\beta)] \in \mathrm{Cl}(\mathfrak{f})$ is of order 3. Indeed, $\beta = 6\sqrt{-7} + 7$ satisfies these conditions.

https://doi.org/10.1017/S0308210516000263 Published online by Cambridge University Press

Since $\beta = 12\theta + 13$, the special value

$$\gamma = \frac{g_{\left[\begin{smallmatrix} 12/5 \\ 13/5 \end{smallmatrix}\right]}(\theta)}{g_{\left[\begin{smallmatrix} 0 \\ 1/5 \end{smallmatrix}\right]}(\theta)}$$

generates $K_{(5)}$ over K by theorem 5.4.

Since the function

$$\frac{g_{\left[\begin{smallmatrix} 12/5 \\ 13/5 \end{smallmatrix}\right]}(\tau)}{g_{\left[\begin{smallmatrix} 0 \\ 1/5 \end{smallmatrix}\right]}(\tau)}$$

belongs to $\mathcal{F}_{25}$ by proposition 3.1, in order to estimate the minimal polynomial of γ over $\mathbb{Q}$ we need to describe the action of $\mathrm{Gal}(K_{(25)}/K)$. Since

$$[K_{(25)}{:}K] = 300 \quad \text{and} \quad [K_{(5)}{:}K] = 12,$$

we have

$$\prod_{\tau \in \mathrm{Gal}(K_{(25)}/K)} (X - \gamma^{\tau}) = \min(\gamma, K)^{25},$$

and hence we can find all conjugates of γ over K in a similar way as in (i). The minimal polynomial of γ over $\mathbb{Q}$ is thus

$$\begin{aligned} \min(\gamma, \mathbb{Q}) = X^{24} &- 3X^{23} + 3X^{22} - 3X^{21} + 11X^{20} - 3X^{19} + 24X^{18} - 24X^{17} \\ &+ 4X^{16} - 18X^{15} + 53X^{14} - 39X^{13} - 11X^{12} - 39X^{11} + 53X^{10} \\ &- 18X^{9} + 4X^{8} - 24X^{7} + 24X^{6} \\ &- 3X^{5} + 11X^{4} - 3X^{3} + 3X^{2} - 3X + 1. \end{aligned}$$

On the other hand, the Siegel–Ramachandra invariant

$$g_{\mathfrak{f}}(C_0) = g_{\left[\begin{smallmatrix} 0 \\ 1/5 \end{smallmatrix}\right]}(\theta)^{60}$$

also generates $K_{(5)}$ over K by theorem 4.6, and its minimal polynomial over K is

$$\begin{aligned} &\min\left(g_{\left[\begin{smallmatrix} 0 \\ 1/5 \end{smallmatrix}\right]}(\theta)^{60}, K\right) \\ &\quad = X^{12} - 531\,770\,250X^{11} + 52\,496\,782\,397\,690\,625X^{10} \\ &\qquad + 12\,347\,712\,418\,332\,056\,278\,906\,250X^{9} \\ &\qquad + 517\,064\,715\,767\,117\,085\,870\,064\,453\,125\,000X^{8} \\ &\qquad + 5\,105\,793\,070\,560\,695\,709\,489\,861\,859\,357\,910\,156\,250X^{7} \\ &\qquad + 30\,043\,009\,324\,891\,990\,472\,511\,274\,397\,078\,094\,482\,421\,875X^{6} \\ &\qquad + 356\,967\,020\,673\,816\,044\,809\,943\,223\,760\,162\,353\,515\,625\,000X^{5} \\ &\qquad + 5\,338\,772\,150\,500\,577\,473\,141\,088\,454\,029\,560\,089\,111\,328\,125X^{4} \end{aligned}$$

$$+\,263\,440\,400\,470\,778\,826\,352\,188\,828\,480\,243\,682\,861\,328\,125X^3$$
$$-\,4\,471\,591\,562\,072\,879\,160\,572\,290\,420\,532\,226\,562\,500X^2$$
$$+\,62\,983\,472\,112\,150\,751\,054\,286\,956\,787\,109\,375X$$
$$+\,931\,322\,574\,615\,478\,515\,625.$$

EXAMPLE 5.9. Let $K = \mathbb{Q}(\sqrt{-5})$ and $\theta = \sqrt{-5}$. Then the class number h_K is 2.

(i) Let $\mathfrak{f} = 4\mathcal{O}_K$. Then 2 is ramified in K, and hence $|\boldsymbol{G}_i| > 2$ for every i. Since $\boldsymbol{G} \cong W_{4,\theta}/\{\pm I_2\}$ and

$$W_{4,\theta}/\{\pm I_2\} = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 2 \\ 2 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 3 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 2 & 3 \\ 1 & 2 \end{bmatrix} \right\},$$

one can check by using propositions 2.3 and 3.2 that the ray class $C' = [(3\sqrt{-5}+2)]$ in $\mathrm{Cl}(\mathfrak{f})$ is of order 2 and satisfies

$$\left(\frac{g_{\mathfrak{f}}(C')}{g_{\mathfrak{f}}(C_0)}\right)^{\sigma(C)} \neq \frac{g_{\mathfrak{f}}(C')}{g_{\mathfrak{f}}(C_0)}$$

for every $C \in \boldsymbol{G} \setminus \{1\}$. Thus, we see from remark 5.6 that

$$K_{(4)} = K\left(\frac{g_{\mathfrak{f}}(C')}{g_{\mathfrak{f}}(C_0)}\right).$$

Furthermore, since $N_{K/\mathbb{Q}}(3\sqrt{-5}+2) \equiv 1 \pmod{48}$, the special value

$$\gamma = \frac{g_{\left[\begin{smallmatrix} 3/4 \\ 2/4 \end{smallmatrix}\right]}(\theta)^4}{g_{\left[\begin{smallmatrix} 0 \\ 1/4 \end{smallmatrix}\right]}(\theta)^4}$$

also generates $K_{(4)}$ over K.

Now that the function

$$\frac{g_{\left[\begin{smallmatrix} 3/4 \\ 2/4 \end{smallmatrix}\right]}(\tau)^4}{g_{\left[\begin{smallmatrix} 0 \\ 1/4 \end{smallmatrix}\right]}(\tau)^4}$$

lies in $\mathcal{F}_8$ by proposition 3.1, in order to estimate the minimal polynomial of γ over $\mathbb{Q}$ we need to know the action of $\mathrm{Gal}(K_{(8)}/K)$. The form class group $C(d_K)$ of discriminant $d_K = -20$ consists of two reduced quadratic forms,

$$Q_1 = [1, 0, 5] \quad \text{and} \quad Q_2 = [2, 2, 3].$$

Thus, we have

$$\theta_{Q_1} = \sqrt{-5},\ \beta_{Q_1} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad \text{and} \quad \theta_{Q_2} = \frac{-1+\sqrt{-5}}{2},\ \beta_{Q_2} = \begin{bmatrix} -1 & -3 \\ 1 & 0 \end{bmatrix}.$$

Then $W_{8,\theta}/\{\pm I_2\}$ and $C(d_K)$ determine the group $\mathrm{Gal}(K_{(8)}/K)$ by proposition 2.4. It follows from proposition 4.1 that

$$[K_{(8)}{:}K] = 32 \quad \text{and} \quad [K_{(4)}{:}K] = 8,$$

https://doi.org/10.1017/S0308210516000263 Published online by Cambridge University Press

and so we attain

$$\prod_{\tau\in\mathrm{Gal}(K_{(8)}/K)}(X-\gamma^\tau)=\min(\gamma,K)^4.$$

Therefore, the minimal polynomial of γ over $\mathbb{Q}$ is

$$\begin{aligned}\min(\gamma,\mathbb{Q})&=X^{16}+3\,024X^{14}+128\,700X^{12}+53\,296X^{10}\\&\quad-124\,026X^8+53\,296X^6+128\,700X^4+3\,024X^2+1.\end{aligned}$$

On the other hand, we deduce that

$$\begin{aligned}&\min\left(g_{\left[\begin{smallmatrix}0\\1/4\end{smallmatrix}\right]}(\theta)^{48},K\right)\\&\quad=X^8-1\,597\,237\,832\,768X^7-15\,846\,881\,298\,723\,072X^6\\&\qquad-26\,992\,839\,895\,872\,106\,496X^5+655\,492\,492\,138\,238\,044\,037\,120X^4\\&\qquad-169\,817\,799\,503\,383\,057\,556\,832\,256X^3\\&\qquad-20\,680\,171\,763\,956\,163\,581\,837\,312X^2\\&\qquad-2\,550\,974\,942\,361\,763\,927\,031\,808X+16\,777\,216.\end{aligned}$$

(ii) Let $\mathfrak{f}=5\mathcal{O}_K$. Then 5 is ramified in K, and hence $|\boldsymbol{G}_i|>2$ for every i. Since 5 divides $d_K=-20$, the special value

$$\gamma=\frac{g_{\left[\begin{smallmatrix}6/5\\1/5\end{smallmatrix}\right]}(\theta)}{g_{\left[\begin{smallmatrix}0\\1/5\end{smallmatrix}\right]}(\theta)}$$

generates $K_{(5)}$ over K by corollary 5.7.

It then follows from propositions 3.1 and 4.1 that

$$\frac{g_{\left[\begin{smallmatrix}6/5\\1/5\end{smallmatrix}\right]}(\tau)}{g_{\left[\begin{smallmatrix}0\\1/5\end{smallmatrix}\right]}(\tau)}\in\mathcal{F}_{25}$$

and

$$[K_{(25)}:K]=500\quad\text{and}\quad[K_{(5)}:K]=20.$$

We deduce that

$$\prod_{\tau\in\mathrm{Gal}(K_{(25)}/K)}(X-\gamma^\tau)=\min(\gamma,K)^{25}.$$

Observe that

$$\theta_{Q_1}=\sqrt{-5},\ \beta_{Q_1}=\begin{bmatrix}1&0\\0&1\end{bmatrix}\quad\text{and}\quad\theta_{Q_2}=\frac{-1+\sqrt{-5}}{2},\ \beta_{Q_2}=\begin{bmatrix}2&1\\0&1\end{bmatrix}$$

in this case. Therefore, we obtain the minimal polynomial of γ over $\mathbb{Q}$ as follows:

$$\begin{aligned}\min(\gamma,\mathbb{Q}) = X^{40} &+ 10X^{39} + 50X^{38} + 170X^{37} + 420X^{36} + 732X^{35} + 965X^{34}\\ &+ 1\,380X^{33} + 2\,545X^{32} + 4\,460X^{31} + 6\,798X^{30} + 7\,880X^{29}\\ &+ 1\,605X^{28} - 11\,800X^{27} - 11\,035X^{26} + 15\,554X^{25}\\ &+ 31\,975X^{24} + 3\,050X^{23} - 29\,125X^{22} - 20\,050X^{21}\\ &- 2\,145X^{20} - 20\,050X^{19} - 29\,125X^{18} + 3\,050X^{17}\\ &+ 31\,975X^{16} + 15\,554X^{15} - 11\,035X^{14} - 11\,800X^{13}\\ &+ 1\,605X^{12} + 7\,880X^{11} + 6\,798X^{10} + 4\,460X^{9} + 2\,545X^{8}\\ &+ 1\,380X^{7} + 965X^{6} + 732X^{5} + 420X^{4} + 170X^{3}\\ &+ 50X^{2}10X + 1.\end{aligned}$$

6. Application to quadratic Diophantine equations

Let n be a square-free positive integer, $K = \mathbb{Q}(\sqrt{-n})$ and θ be as in (2.3). We assume $-n \equiv 2, 3 \pmod 4$, so that $d_K \equiv 0 \pmod 4$ and $\mathcal{O}_K = \mathbb{Z}[\sqrt{-n}]$. By means of ray-class invariants over K, Cho [1] provided a criterion for whether a given odd prime p can be written in the form $p = x^2 + ny^2$ for some $x, y \in \mathbb{Z}$ with additional conditions $x \equiv 1 \pmod N$, $y \equiv 0 \pmod N$ for each positive integer N.

PROPOSITION 6.1. *For a positive integer N, we let $f_N(X) \in \mathbb{Z}[X]$ be the minimal polynomial of a real algebraic integer that generates $K_{(N)}$ over K. If an odd prime p divides neither nN nor the discriminant of $f_N(X)$, then*

$$\begin{aligned}&p = x^2 + ny^2 \text{ with } x, y \in \mathbb{Z},\ x \equiv 1 \pmod N,\ y \equiv 0 \pmod N\\ &\qquad\iff \left(\frac{-n}{p}\right) = 1 \text{ and } f_N(X) \equiv 0 \pmod p \text{ has an integer solution,}\end{aligned}$$

where $(-n/p)$ is the Kronecker symbol.

Proof. See [1, theorem 1]. □

LEMMA 6.2. *Let $N \geqslant 2$ be an integer.*

(i) *For $s \in \mathbb{Z} \setminus N\mathbb{Z}$,*

$$\frac{g_{\left[\begin{smallmatrix}0\\ s/N\end{smallmatrix}\right]}(\theta)}{g_{\left[\begin{smallmatrix}0\\ 1/N\end{smallmatrix}\right]}(\theta)}$$

is a real number.

(ii) *For $t \in \mathbb{Z}$,*

$$\mathrm{i}e^{(t/2N)\pi \mathrm{i}}\frac{g_{\left[\begin{smallmatrix}1/2\\ t/N\end{smallmatrix}\right]}(\theta)}{g_{\left[\begin{smallmatrix}0\\ 1/N\end{smallmatrix}\right]}(\theta)}$$

is a real number.

https://doi.org/10.1017/S0308210516000263 Published online by Cambridge University Press

Proof. We obtain, by definition,

$$\begin{aligned}
\mathrm{e}^{(t/2N)\pi\mathrm{i}} g_{\left[\begin{smallmatrix}1/2\\ t/N\end{smallmatrix}\right]}(\theta) &= -q_\theta^{\boldsymbol{B}_2(1/2)/2}(1-q_\theta^{1/2}\zeta_N^t)\prod_{n=1}^{\infty}(1-q_\theta^{n+1/2}\zeta_N^t)(1-q_\theta^{n-1/2}\zeta_N^{-t}) \\
&= -q_\theta^{\boldsymbol{B}_2(1/2)/2}\prod_{n=0}^{\infty}(1-q_\theta^{n+1/2}\zeta_N^t)\prod_{n=1}^{\infty}(1-q_\theta^{n-1/2}\zeta_N^{-t}) \\
&= -q_\theta^{\boldsymbol{B}_2(1/2)/2}\prod_{n=1}^{\infty}(1-q_\theta^{n-1/2}\zeta_N^t)(1-q_\theta^{n-1/2}\zeta_N^{-t}) \\
&= -q_\theta^{\boldsymbol{B}_2(1/2)/2}\prod_{n=1}^{\infty}\{1-q_\theta^{n-1/2}(\zeta_N^t+\zeta_N^{-t})+q_\theta^{2n-1}\},
\end{aligned}$$

and we deduce that

$$\begin{aligned}
-ig_{\left[\begin{smallmatrix}0\\ s/N\end{smallmatrix}\right]}(\theta) &= \mathrm{i}q_\theta^{1/12}\mathrm{e}^{-(s/N)\pi\mathrm{i}}(1-\zeta_N^s)\prod_{n=1}^{\infty}(1-q_\theta^n\zeta_N^s)(1-q_\theta^n\zeta_N^{-s}) \\
&= \mathrm{i}q_\theta^{1/12}(\zeta_{2N}^{-s}-\zeta_{2N}^{s})\prod_{n=1}^{\infty}\{1-q_\theta^n(\zeta_N^s+\zeta_N^{-s})+q_\theta^{2n}\}.
\end{aligned}$$

Since q_θ, $\zeta_N^t+\zeta_N^{-t}$ and $\mathrm{i}(\zeta_{2N}^{-s}-\zeta_{2N}^{s})$ are real numbers, we prove the lemma. □

THEOREM 6.3. *Let N be a positive integer and let $\mathfrak{f}=N\mathcal{O}_K$ with prime ideal factorization*

$$\mathfrak{f}=\prod_{i=1}^{r}\mathfrak{p}_i^{n_i}.$$

Assume that $K_{\mathfrak{f}}\neq K_{\mathfrak{f}\mathfrak{p}_i^{-n_i}}$ and $|\boldsymbol{G}_i|>2$ for every i.

(i) *Let s be an integer prime to N such that the order of $[s]$ in $(\mathbb{Z}/N\mathbb{Z})^\times/\{\pm1\}$ is an odd prime p (if any). If $p>3$ or $|\boldsymbol{G}_i|>3$ for every i, then the special value*

$$\frac{g_{\left[\begin{smallmatrix}0\\ s/N\end{smallmatrix}\right]}(\theta)^m}{g_{\left[\begin{smallmatrix}0\\ 1/N\end{smallmatrix}\right]}(\theta)^m}$$

generates $K_{(N)}$ over K as a real algebraic integer, where m is an integer dividing N for which $m(s^2-1)\equiv 0 \pmod{\gcd(2,N)\cdot N}$ and $m\equiv N \pmod 2$.

(ii) *When N is even, we set $C'=[((N/2)\theta+t)]\in \mathrm{Cl}(\mathfrak{f})$ with $t\in\mathbb{Z}$ such that $t^2\equiv 1 \pmod N$. We further assume that*

$$\left(\frac{g_{\mathfrak{f}}(C')}{g_{\mathfrak{f}}(C_0)}\right)^{\sigma(C)}\neq\frac{g_{\mathfrak{f}}(C')}{g_{\mathfrak{f}}(C_0)}$$

for every $C\in\boldsymbol{G}\setminus\{1\}$. If 4 divides Nn, then the special value

$$\mathrm{e}^{(2t/N)\pi\mathrm{i}}\frac{g_{\left[\begin{smallmatrix}1/2\\ t/N\end{smallmatrix}\right]}(\theta)^4}{g_{\left[\begin{smallmatrix}0\\ 1/N\end{smallmatrix}\right]}(\theta)^4}$$

https://doi.org/10.1017/S0308210516000263 Published online by Cambridge University Press

is a real algebraic integer and generates $K_{(N)}$ over K. In particular, if 4 divides N, then the special value

$$\mathrm{e}^{(t/N)\pi\mathrm{i}}\frac{g_{\left[\begin{smallmatrix}1/2\\ t/N\end{smallmatrix}\right]}(\theta)^2}{g_{\left[\begin{smallmatrix}0\\ 1/N\end{smallmatrix}\right]}(\theta)^2}$$

also generates $K_{(N)}$ over K as a real algebraic integer.

Proof. (i) Let $C' = [(s)] \in \mathrm{Cl}(\mathfrak{f})$. Then the order of C' in $\mathrm{Cl}(\mathfrak{f})$ is p, and so we see from theorem 5.4 that

$$K_{(N)} = K\left(\frac{g_{\mathfrak{f}}(C')}{g_{\mathfrak{f}}(C_0)}\right),$$

and the function

$$\frac{g_{\left[\begin{smallmatrix}0\\ s/N\end{smallmatrix}\right]}(\tau)^m}{g_{\left[\begin{smallmatrix}0\\ 1/N\end{smallmatrix}\right]}(\tau)^m}$$

lies in $\mathcal{F}_N$, from which we attain

$$\gamma = \frac{g_{\left[\begin{smallmatrix}0\\ s/N\end{smallmatrix}\right]}(\theta)^m}{g_{\left[\begin{smallmatrix}0\\ 1/N\end{smallmatrix}\right]}(\theta)^m} \in K_{(N)}$$

by propositions 2.1 and 3.1. Since $\gamma^{12N/m} = g_{\mathfrak{f}}(C')/g_{\mathfrak{f}}(C_0)$, the special value γ also generates $K_{(N)}$ over K as a real algebraic integer by lemma 6.2. Note that $m = N$ always satisfies the condition $m(s^2-1) \equiv 0 \pmod{\gcd(2, N)\cdot N}$. Indeed, if N is even, then $s^2 - 1$ must be even because s is prime to N.

(ii) Now that

$$\left(\frac{N\theta}{2} + t\right)^2 \equiv -\frac{Nn}{4}N + tN\theta + t^2 \equiv 1 \pmod{N\mathcal{O}_K},$$

the ray class C' is of order 2 in $\mathrm{Cl}(\mathfrak{f})$. Then it follows from remark 5.6 that

$$K_{(N)} = K\left(\frac{g_{\mathfrak{f}}(C')}{g_{\mathfrak{f}}(C_0)}\right),$$

and the function

$$\mathrm{e}^{(2t/N)\pi\mathrm{i}}\frac{g_{\left[\begin{smallmatrix}1/2\\ t/N\end{smallmatrix}\right]}(\tau)^4}{g_{\left[\begin{smallmatrix}0\\ 1/N\end{smallmatrix}\right]}(\tau)^4}$$

lies in $\mathcal{F}_N$, which yields

$$\gamma = \mathrm{e}^{(2t/N)\pi\mathrm{i}}\frac{g_{\left[\begin{smallmatrix}1/2\\ t/N\end{smallmatrix}\right]}(\theta)^4}{g_{\left[\begin{smallmatrix}0\\ 1/N\end{smallmatrix}\right]}(\theta)^4} \in K_{(N)}$$

by propositions 2.1 and 3.1. Since $\gamma^{3N} = g_{\mathfrak{f}}(C')/g_{\mathfrak{f}}(C_0)$, the special value γ also generates $K_{(N)}$ over K and is a real algebraic integer by lemma 6.2.

In particular, if 4 divides N, then we have

$$\mathrm{e}^{(t/N)\pi\mathrm{i}}\frac{g_{\left[\begin{smallmatrix}1/2\\ t/N\end{smallmatrix}\right]}(\tau)^2}{g_{\left[\begin{smallmatrix}0\\ 1/N\end{smallmatrix}\right]}(\tau)^2}\in\mathcal{F}_N$$

by proposition 3.1. And, similarly, we get the conclusion. □

REMARK 6.4. Recently, Jung *et al*. [5] proved that if $N\equiv d_K\equiv 0 \pmod 4$ and $|d_K|\geqslant 4N^{4/3}$, then the ray class $C'=[((\frac{1}{2}N)\theta+(\frac{1}{2}N)+1)]\in \mathrm{Cl}(\mathfrak{f})$ satisfies

$$\left(\frac{g_{\mathfrak{f}}(C')}{g_{\mathfrak{f}}(C_0)}\right)^{\sigma(C)}\neq\frac{g_{\mathfrak{f}}(C')}{g_{\mathfrak{f}}(C_0)}$$

for every $C\in \boldsymbol{G}\setminus\{1\}$. Thus, if $K_{\mathfrak{f}}\neq K_{\mathfrak{f}\mathfrak{p}_i^{-n_i}}$ and $|\boldsymbol{G}_i|>2$ for every i, the special value

$$\mathrm{e}^{(1/2+1/N)\pi\mathrm{i}}\frac{g_{\left[\begin{smallmatrix}1/2\\ 1/2+1/N\end{smallmatrix}\right]}(\theta)^2}{g_{\left[\begin{smallmatrix}0\\ 1/N\end{smallmatrix}\right]}(\theta)^2}$$

generates $K_{(N)}$ over K as a real algebraic integer by theorem 6.3.

COROLLARY 6.5. *Using the notation and assumptions in theorem 6.3, let p be an odd prime satisfying $p^2|N$ (if any). If $p>3$ or $|\boldsymbol{G}_i|>3$ for every i, then the special value*

$$\frac{g_{\left[\begin{smallmatrix}0\\ 1/p+1/N\end{smallmatrix}\right]}(\theta)^m}{g_{\left[\begin{smallmatrix}0\\ 1/N\end{smallmatrix}\right]}(\theta)^m}$$

generates $K_{(N)}$ over K as a real algebraic integer, where

$$m=\begin{cases}p & \text{if } N \text{ is odd},\\ 2p & \text{if } N \text{ is even}.\end{cases}$$

Proof. Let $s=1+N/p$. For a positive integer i, we have

$$s^i\equiv 1+\frac{N}{p}i \pmod N$$

and hence the ray class $[(s)]\in\mathrm{Cl}(\mathfrak{f})$ is of order p and $m(s^2-1)\equiv 0 \pmod{\gcd(2,N)\cdot N}$. Therefore, the corollary follows from theorem 6.3(i). □

Now, we are ready to apply the ray-class invariants in theorem 6.3 to the quadratic Diophantine equations described in proposition 6.1.

EXAMPLE 6.6. Let $K=\mathbb{Q}(\sqrt{-1})$, $\theta=\sqrt{-1}$ and $\mathfrak{f}=9\mathcal{O}_K$. Then 3 is inert in K, and hence $|\boldsymbol{G}_i|>3$ for every i. Since the ray class $C'=[(4)]$ in $\mathrm{Cl}(\mathfrak{f})$ is of order 3, the special value

$$\gamma=\frac{g_{\left[\begin{smallmatrix}0\\ 4/9\end{smallmatrix}\right]}(\theta)^3}{g_{\left[\begin{smallmatrix}0\\ 1/9\end{smallmatrix}\right]}(\theta)^3}$$

generates $K_{(9)}$ over K as a real algebraic integer by corollary 6.5. Here we observe that $\mathrm{Gal}(K_{(9)}/K) \cong W_{9,\theta}/\ker(\varphi_{9,\theta})$ by proposition 2.4, and we have

$$\begin{aligned} &W_{9,\theta}/\ker(\varphi_{9,\theta}) \\ &\quad = \left\{ \begin{bmatrix}1&0\\0&1\end{bmatrix}, \begin{bmatrix}0&7\\2&0\end{bmatrix}, \begin{bmatrix}0&5\\4&0\end{bmatrix}, \begin{bmatrix}1&8\\1&1\end{bmatrix}, \begin{bmatrix}1&7\\2&1\end{bmatrix}, \begin{bmatrix}1&6\\3&1\end{bmatrix}, \begin{bmatrix}1&5\\4&1\end{bmatrix}, \begin{bmatrix}1&4\\5&1\end{bmatrix}, \right. \\ &\qquad \begin{bmatrix}1&3\\6&1\end{bmatrix}, \begin{bmatrix}1&2\\7&1\end{bmatrix}, \begin{bmatrix}2&7\\2&2\end{bmatrix}, \begin{bmatrix}2&6\\3&2\end{bmatrix}, \begin{bmatrix}2&5\\4&2\end{bmatrix}, \begin{bmatrix}2&4\\5&2\end{bmatrix}, \begin{bmatrix}2&3\\6&2\end{bmatrix}, \begin{bmatrix}3&5\\4&3\end{bmatrix}, \\ &\qquad \left. \begin{bmatrix}3&4\\5&3\end{bmatrix}, \begin{bmatrix}4&5\\4&4\end{bmatrix} \right\}, \end{aligned}$$

where $\varphi_{9,\theta}$ is the homomorphism stated in proposition 2.2. Hence, we obtain the minimal polynomial $f_9(X)$ of γ over K as

$$\begin{aligned} f_9(X) = X^{18} &- 36X^{17} + 234X^{16} + 1\,086X^{15} + 2\,547X^{14} + 12\,294X^{13} \\ &+ 32\,415X^{12} + 41\,976X^{11} + 45\,459X^{10} + 55\,748X^{9} + 51\,480X^{8} \\ &+ 22\,914X^{7} - 1\,092X^{6} - 5\,310X^{5} - 1\,719X^{4} + 6X^{3} \\ &+ 99X^{2} + 18X + 1 \end{aligned}$$

and so we achieve $\mathrm{disc}(f_9(X)) = 2^{54} \cdot 3^{135} \cdot 127^{6} \cdot 827^{2}$. On the other hand, an odd prime p satisfies $(-1/p) = 1$ if and only if $p \equiv 1 \pmod 4$. Therefore, if $p \neq 2, 3, 127, 827$, we see by proposition 6.1 that a prime p can be expressed as $p = x^2 + y^2$ for some $x, y \in \mathbb{Z}$ with conditions $x \equiv 1 \pmod 9$, $y \equiv 0 \pmod 9$ if and only if $p \equiv 1 \pmod 4$ and $f_9(X) \equiv 0 \pmod p$ has an integer solution.

Example 6.7. Let $K = \mathbb{Q}(\sqrt{-5})$, $\theta = \sqrt{-5}$ and $\mathfrak{f} = 4\mathcal{O}_K$. Then 2 is ramified in K and so $|\boldsymbol{G}_i| > 2$ for every i. In a similar way as in example 5.9 one can show that the ray class $C' = [(2\sqrt{-5} + 1)] \in \mathrm{Cl}(\mathfrak{f})$ satisfies

$$\left(\frac{g_{\mathfrak{f}}(C')}{g_{\mathfrak{f}}(C_0)}\right)^{\sigma(C)} \neq \frac{g_{\mathfrak{f}}(C')}{g_{\mathfrak{f}}(C_0)}$$

for every $C \in \boldsymbol{G} \setminus \{1\}$. Thus, the special value

$$\gamma = \mathrm{e}^{\pi \mathrm{i}/4} \frac{g_{\left[\begin{smallmatrix}1/2\\1/4\end{smallmatrix}\right]}(\theta)^2}{g_{\left[\begin{smallmatrix}0\\1/4\end{smallmatrix}\right]}(\theta)^2}$$

generates $K_{(4)}$ over K as a real algebraic integer by theorem 6.3, and we get the minimal polynomial $f_4(X)$ of γ over K as follows:

$$f_4(X) = X^8 + 16X^7 - 12X^6 + 16X^5 + 38X^4 - 16X^3 - 12X^2 - 16X + 1.$$

On the other hand, the discriminant of $f_4(X)$ is $2^{68} \cdot 5^4$ and we derive that an odd prime p satisfies $(-5/p) = 1$ if and only if $p \equiv 1, 3, 7, 9 \pmod{20}$. Therefore, if $p \neq 2, 5$ we conclude that a prime p can be written in the form $p = x^2 + 5y^2$ for some $x, y \in \mathbb{Z}$ with conditions $x \equiv 1 \pmod 4$, $y \equiv 0 \pmod 4$ if and only if $p \equiv 1, 3, 7, 9 \pmod{20}$ and $X^8 + 16X^7 - 12X^6 + 16X^5 + 38X^4 - 16X^3 - 12X^2 - 16X + 1 \equiv 0 \pmod p$ has an integer solution.

https://doi.org/10.1017/S0308210516000263 Published online by Cambridge University Press

Acknowledgements

We thank the referee for valuable comments that significantly improved the paper.

References

1 B. Cho. Primes of the form x^2+ny^2 with conditions $x \equiv 1 \bmod N$, $y \equiv 0 \bmod N$. *J. Number Theory* **130** (2010), 852–861.

2 D. A. Cox. *Primes of the form x^2+ny^2: Fermat, class field, and complex multiplication* (New York: Wiley Interscience, 1989).

3 A. Gee and P. Stevenhagen. Generating class fields using Shimura reciprocity. In *Algorithmic number theory*. Lecture Notes in Computer Science, vol. 1423, pp. 441–453 (Springer, 1998).

4 G. J. Janusz. *Algebraic number fields*, 2nd edn. Graduate Studies in Mathematics, vol. 7 (Providence, RI: American Mathematical Society, 1996).

5 H. Y. Jung, J. K. Koo and D. H. Shin. On some Fricke families and application to the Lang–Schertz conjecture. *Proc. R. Soc. Edinb.* A **146** (2016), 723–740.

6 D. Kubert and S. Lang. *Modular units*. Grundlehren der mathematischen Wissenschaften, vol. 244 (Spinger, 1981).

7 S. Lang. *Elliptic functions*, 2nd edn (Spinger, 1987).

8 S. Lang. *Algebraic number theory*, 2nd edn. Graduate Texts in Mathematics, vol. 110 (Springer, 1994).

9 F. Lemmermeyer. Conics: a poor man's elliptic curves. Preprint, 2003. (Available at https://arxiv.org/abs/math/0311306.)

10 K. Ramachandra. Some applications of Kronecker's limit formulas. *Annals Math. (2)* **80** (1964), 104–148.

11 R. Schertz. Construction of ray class fields by elliptic units. *J. Théorie Nombres Bordeaux* **9** (1997), 383–394.

12 R. Schertz. *Complex multiplication*, New Mathematics Monographs, vol. 15 (Cambridge University Press, 2010).

13 J.-P. Serre. *A course in arithmetic*. Graduate Texts in Mathematics, vol. 7 (Springer, 1973).

14 G. Shimura. *Introduction to the arithmetic theory of automorphic functions* (Princeton University Press, 1994).

15 C. L. Siegel. *Lectures on advanced analytic number theory*, Tata Institute of Fundamental Research Lectures on Mathematics, vol. 23 (Bombay: Tata Institute of Fundamental Research, 1965).

16 P. Stevenhagen. Hilbert's 12th problem, complex multiplication and Shimura reciprocity. In *Class field theory: its centenary and prospect*. Advanced Studies in Pure Mathematics, vol. 30, pp. 161–176 (Tokyo: Mathematical Society of Japan, 2001).