Proceedings of the Royal Society of Edinburgh, **146A**, 723–740, *2016*
DOI:10.1017/S0308210515000608

On some Fricke families and application to the Lang–Schertz conjecture

Ho Yun Jung
National Institute for Mathematical Sciences, Daejeon 305-811, Republic of Korea (hoyunjung@nims.re.kr)

Ja Kyung Koo
Department of Mathematical Sciences, KAIST, Daejeon 305-701, Republic of Korea (jkkoo@math.kaist.ac.kr)

Dong Hwa Shin*
Department of Mathematics, Hankuk University of Foreign Studies, Yongin-si, Gyeonggi-do 449-791, Republic of Korea (dhshin@hufs.ac.kr)

(MS received 4 November 2014; accepted 11 March 2015)

We investigate two kinds of Fricke families, those consisting of Fricke functions and those consisting of Siegel functions. In terms of their special values we then generate ray class fields of imaginary quadratic fields over the Hilbert class fields, which are related to the Lang–Schertz conjecture.

Keywords: complex multiplication; Fricke families; modular functions

2010 *Mathematics subject classification:* Primary 11G15
Secondary 11F03

1. Introduction

For a positive integer N let $\mathcal{F}_N$ be the field of all meromorphic modular functions of level N whose Fourier coefficients lie in the Nth cyclotomic field $\mathbb{Q}(\zeta_N)$ with $\zeta_N = \mathrm{e}^{2\pi\mathrm{i}/N}$. Then it is well known that $\mathcal{F}_1$ is generated over $\mathbb{Q}$ by the elliptic modular function

$$j(\tau) = 1/q + 744 + 196884q + 21493760q^2 + \cdots \quad (\tau \in \mathbb{H},\ \text{the complex upper half-plane}),$$

where $q = \mathrm{e}^{2\pi\mathrm{i}\tau}$. Furthermore, $\mathcal{F}_N$ is a Galois extension of $\mathcal{F}_1$, whose Galois group is isomorphic to $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I_2\}$ (see [9, §§ 6.1 and 6.2]).

For $N \geqslant 2$ we let

$$\mathcal{V}_N = \{\boldsymbol{v} \in \mathbb{Q}^2 \mid \boldsymbol{v} \text{ has primitive denominator } N\},$$

*Corresponding author.

that is, $\boldsymbol{v} \in \mathbb{Q}^2$ belongs to $\mathcal{V}_N$ if and only if N is the smallest positive integer satisfying $N\boldsymbol{v} \in \mathbb{Z}^2$. We call a family $\{h_{\boldsymbol{v}}(\tau)\}_{\boldsymbol{v}\in\mathcal{V}_N}$ of functions in $\mathcal{F}_N$ a *Fricke family of level* N if

(F1) $h_{\boldsymbol{v}}(\tau)$ is weakly holomorphic (namely, $h_{\boldsymbol{v}}(\tau)$ is holomorphic on $\mathbb{H}$);

(F2) $h_{\boldsymbol{v}}(\tau)$ depends only on $\pm\boldsymbol{v} \pmod{\mathbb{Z}^2}$;

(F3) $h_{\boldsymbol{v}}(\tau)^\gamma = h_{{}^t\gamma\boldsymbol{v}}(\tau)$ for all $\gamma \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I_2\} \simeq \mathrm{Gal}(\mathcal{F}_N/\mathcal{F}_1)$, where ${}^t\gamma$ indicates the transpose of γ.

In this paper we deal with two kinds of Fricke families,

$$\{f_{\boldsymbol{v}}(\tau)\}_{\boldsymbol{v}\in\mathcal{V}_N} \quad \text{and} \quad \{g_{\boldsymbol{v}}(\tau)^{12N}\}_{\boldsymbol{v}\in\mathcal{V}_N},$$

one consisting of Fricke functions and the other consisting of $12N$th powers of Siegel functions (see § 2).

Let K be an imaginary quadratic field of discriminant d_K other than $\mathbb{Q}(\sqrt{-1})$ and $\mathbb{Q}(\sqrt{-3})$, and let $\mathfrak{n}$ be a proper non-trivial ideal of the ring of integers $\mathcal{O}_K$ of K. Furthermore, let N (greater than or equal to 2) be the smallest positive integer in $\mathfrak{n}$ and let C be a ray class in the ray class group $\mathrm{Cl}(\mathfrak{n})$ of K modulo $\mathfrak{n}$. For a Fricke family $\{h_{\boldsymbol{v}}(\tau)\}_{\boldsymbol{v}\in\mathcal{V}_N}$ of level N we shall define in § 3 the *Fricke invariant* $h_{\mathfrak{n}}(C)$, which depends only on $\mathfrak{n}$ and C. The first main theorem of this paper then asserts that $f_{\mathfrak{n}}(C)$ generates the ray class field $K_{\mathfrak{n}}$ of K modulo $\mathfrak{n}$ over the Hilbert class field H_K of K (see theorem 3.2).

On the other hand, Lang [5, p. 292] and Schertz [7] conjectured that $g_{\mathfrak{n}}^{12N}(C)$, which is called the *Siegel–Ramachandra invariant* modulo $\mathfrak{n}$ at C, generates $K_{\mathfrak{n}}$ over H_K (in fact, even over K). See also [1] and [8]. Recently, Cho [2] gave a conditional proof by adopting Schertz's idea and using the second Kronecker limit formula as follows. Let $\mathfrak{n} = \prod_{k=1}^r \mathfrak{p}_k^{e_k}$ be the prime ideal factorization of $\mathfrak{n}$. If the exponent of the quotient group $(\mathcal{O}_K/\mathfrak{p}_k^{e_k})^\times/\{\alpha + \mathfrak{p}_k^{e_k} \mid \alpha \in \mathcal{O}_K^\times\}$ is greater than 2 for every $k = 1, \ldots, r$, then $g_{\mathfrak{n}}^{12N}(C)$ generates $K_{\mathfrak{n}}$ over K.

As the second main theorem, we present a new conditional proof of the Lang–Schertz conjecture (theorem 4.1 and corollary 4.3). We furthermore show that the $6N$th root, which will give a relatively small power, of a certain quotient of Siegel–Ramachandra invariants generates $K_{\mathfrak{n}}$ over H_K when $d_K \equiv N \equiv 0 \pmod 4$, $|d_K| \geqslant 4N^{4/3}$ and $\mathfrak{n} = N\mathcal{O}_K$ (theorem 6.2). To this end, we shall find some relations between Fricke and Siegel functions (lemma 2.5), and make use of an explicit version of Shimura's reciprocity law due to Stevenhagen (proposition 5.2). Finally, we note that these invariants have minimal polynomials with (relatively) small coefficients (example 6.4).

2. Fricke families

Let Λ be a lattice in $\mathbb{C}$. The *Weierstrass* $\wp$*-function* relative to Λ is defined by

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

Then it is a meromorphic function on z and is periodic with respect to Λ.

LEMMA 2.1. *If $z_1, z_2 \in \mathbb{C} \setminus \Lambda$, then $\wp(z_1;\Lambda) = \wp(z_2;\Lambda)$ if and only if $z_1 \equiv \pm z_2 \pmod{\Lambda}$.*

Proof. See [10, ch. IV, § 3]. □

Let N (greater than or equal to 2) be an integer and let $\boldsymbol{v} = \left[\begin{smallmatrix} v_1 \\ v_2 \end{smallmatrix}\right] \in \mathcal{V}_N$. We define

$$\wp_{\boldsymbol{v}}(\tau) = \wp(v_1\tau + v_2; [\tau, 1]) \quad (\tau \in \mathbb{H}), \tag{2.1}$$

which is a weakly holomorphic modular form of level N and weight 2 [5, ch. 6]. We furthermore define auxiliary functions $g_2(\tau)$, $g_3(\tau)$ and $\Delta(\tau)$ on $\mathbb{H}$ by

$$g_2(\tau) = 60 \sum_{\omega \in [\tau,1]\setminus\{0\}} \frac{1}{\omega^4}, \qquad g_3(\tau) = 140 \sum_{\omega \in [\tau,1]\setminus\{0\}} \frac{1}{\omega^6}$$

and

$$\Delta(\tau) = g_2(\tau)^3 - 27 g_3(\tau)^2,$$

which are holomorphic modular forms of level 1 and weight 4, 6 and 12, respectively (see [5, ch. 3, § 2]). Now, we define the *Fricke function* (or the *first Weber function*) $f_{\boldsymbol{v}}(\tau)$ by

$$f_{\boldsymbol{v}}(\tau) = -2^7 3^5 \frac{g_2(\tau) g_3(\tau)}{\Delta(\tau)} \wp_{\boldsymbol{v}}(\tau) \quad (\tau \in \mathbb{H}). \tag{2.2}$$

PROPOSITION 2.2. *The family $\{f_{\boldsymbol{v}}(\tau)\}_{\boldsymbol{v} \in \mathcal{V}_N}$ is a Fricke family of level N.*

Proof. See [5, ch. 6, §§ 2 and 3]. □

The *Weierstrass σ-function* relative to Λ is defined by

$$\sigma(z;\Lambda) = z \prod_{\omega \in \Lambda\setminus\{0\}} \left(1 - \frac{z}{\omega}\right) \mathrm{e}^{z/\omega + \frac{1}{2}(z/\omega)^2} \quad (z \in \mathbb{C}).$$

Taking the logarithmic derivative we obtain the *Weierstrass ζ-function* as

$$\zeta(z;\Lambda) = \frac{\sigma'(z;\Lambda)}{\sigma(z;\Lambda)} = \frac{1}{z} + \sum_{\omega \in \Lambda\setminus\{0\}} \left(\frac{1}{z-\omega} + \frac{1}{\omega} + \frac{z}{\omega^2}\right).$$

Since $\zeta'(z;\Lambda) = -\wp(z;\Lambda)$ is periodic with respect to Λ, for any $\omega \in \Lambda$ there is a constant $\eta(\omega;\Lambda)$ so that

$$\zeta(z+\omega;\Lambda) - \zeta(z;\Lambda) = \eta(\omega;\Lambda).$$

Next we define the *Siegel function* $g_{\boldsymbol{v}}(\tau)$ by

$$g_{\boldsymbol{v}}(\tau) = \exp\{-\tfrac{1}{2}(v_1\eta(\tau;[\tau,1]) + v_2\eta(1;[\tau,1]))(v_1\tau + v_2)\}\sigma(v_1\tau + v_2;[\tau,1])\eta(\tau)^2 \quad (\tau \in \mathbb{H}),$$

where

$$\eta(\tau) = \sqrt{2\pi}\zeta_8 q^{1/24} \prod_{n=1}^{\infty}(1-q^n) \quad (q = \mathrm{e}^{2\pi\mathrm{i}\tau},\ \tau \in \mathbb{H})$$

is the *Dedekind* η*-function*. By the product formula of the Weierstrass σ-function we obtain the q-product expression

$$g_{\boldsymbol{v}}(\tau) = -\mathrm{e}^{\pi \mathrm{i} v_2(v_1-1)} q^{\frac{1}{2}B_2(v_1)}(1-q^{v_1}\mathrm{e}^{2\pi\mathrm{i}v_2}) \times \prod_{n=1}^{\infty}(1-q^{n+v_1}\mathrm{e}^{2\pi\mathrm{i}v_2})(1-q^{n-v_1}\mathrm{e}^{-2\pi\mathrm{i}v_2}), \tag{2.3}$$

where $B_2(X) = X^2 - X + 1/6$ is the second Bernoulli polynomial (see [5, ch. 18, theorem 4 and ch. 19, § 2]). Furthermore, we have the q-order formula

$$\mathrm{ord}_q(g_{\boldsymbol{v}}(\tau)) = \tfrac{1}{2}B_2(\langle v_1\rangle), \tag{2.4}$$

where $\langle X\rangle$ is the fractional part of $X \in \mathbb{R}$ such that $0 \leqslant \langle X\rangle < 1$ (see [4, ch. 2, § 1]).

Lemma 2.3. *Let* $\{m(\boldsymbol{v})\}_{\boldsymbol{v}=\left[\begin{smallmatrix} v_1\\ v_2\end{smallmatrix}\right]\in\mathcal{V}_N}$ *be a family of integers such that* $m(\boldsymbol{v}) = 0$ *except for finitely many* $\boldsymbol{v}$. *If the family satisfies*

$$\sum_{\boldsymbol{v}} m(\boldsymbol{v})(Nv_1)^2 \equiv \sum_{\boldsymbol{v}} m(\boldsymbol{v})(Nv_2)^2 \equiv 0 \pmod{\gcd(2,N)\cdot N},$$
$$\sum_{\boldsymbol{v}} m(\boldsymbol{v})(Nv_1)(Nv_2) \equiv 0 \pmod{N},$$
$$\gcd(12,N)\sum_{\boldsymbol{v}} m(\boldsymbol{v}) \equiv 0 \pmod{12},$$

then $\zeta\prod_{\boldsymbol{v}} g_{\boldsymbol{v}}(\tau)^{m(\boldsymbol{v})}$ *belongs to* $\mathcal{F}_N$, *where* $\zeta = \prod_{\boldsymbol{v}} \mathrm{e}^{\pi\mathrm{i}v_2(1-v_1)m(\boldsymbol{v})} \in \mathbb{Q}(\zeta_{2N^2})$.

Proof. See [4, ch. 3, theorems 5.2 and 5.3] and (2.3). □

Proposition 2.4. *The family* $\{g_{\boldsymbol{v}}(\tau)^{12N}\}_{\boldsymbol{v}\in\mathcal{V}_N}$ *is a Fricke family of level* N.

Proof. See [4, ch. 2, proposition 1.3]. □

Lemma 2.5. *We further obtain the following results on modular functions.*

(i) *If* $h(\tau)$ *is a weakly holomorphic function in* $\mathcal{F}_1$, *then it is a polynomial in* $j(\tau)$ *over* $\mathbb{Q}$.

(ii) *We have* $\mathcal{F}_1\Big(f_{\left[\begin{smallmatrix} 0\\ 1/N\end{smallmatrix}\right]}(\tau)\Big) = \mathcal{F}_1\Big(g_{\left[\begin{smallmatrix} 0\\ 1/N\end{smallmatrix}\right]}(\tau)^{12N}\Big)$.

(iii) *We get the relation*

$$f_{\left[\begin{smallmatrix} 0\\ 1/N\end{smallmatrix}\right]}(\tau) = \frac{p\Big(j(\tau), g_{\left[\begin{smallmatrix} 0\\ 1/N\end{smallmatrix}\right]}(\tau)^{12N}\Big)}{\mathrm{disc}\Big(g_{\left[\begin{smallmatrix} 0\\ 1/N\end{smallmatrix}\right]}(\tau)^{12N}, \mathcal{F}_1\Big)}$$

for some polynomial $p(X,Y) \in \mathbb{Q}[X,Y]$.

Proof.
(i) See [5, ch. 5, theorem 2].

(ii) Let

$$L = \mathcal{F}_1\Big(f_{\left[\begin{smallmatrix} 0 \\ 1/N \end{smallmatrix}\right]}(\tau)\Big) \quad \text{and} \quad R = \mathcal{F}_1\Big(g_{\left[\begin{smallmatrix} 0 \\ 1/N \end{smallmatrix}\right]}(\tau)^{12N}\Big),$$

which are intermediate subfields of the extension $\mathcal{F}_N/\mathcal{F}_1$ by propositions 2.2 and 2.4. Let $\gamma = \left[\begin{smallmatrix} x & y \\ z & w \end{smallmatrix}\right] \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I_2\} \simeq \mathrm{Gal}(\mathcal{F}_N/\mathcal{F}_1)$. We then deduce that

$$\begin{aligned}
\gamma \in \mathrm{Gal}(\mathcal{F}_N/L) &\iff f_{\left[\begin{smallmatrix} 0 \\ 1/N \end{smallmatrix}\right]}(\tau)^{\gamma} = f_{\left[\begin{smallmatrix} 0 \\ 1/N \end{smallmatrix}\right]}(\tau) \\
&\iff f_{{}^{\mathrm{t}}\gamma\left[\begin{smallmatrix} 0 \\ 1/N \end{smallmatrix}\right]}(\tau) = f_{\left[\begin{smallmatrix} 0 \\ 1/N \end{smallmatrix}\right]}(\tau) \quad \text{by proposition 2.2, (F2) and (F3)} \\
&\iff f_{\left[\begin{smallmatrix} z/N \\ w/N \end{smallmatrix}\right]}(\tau) = f_{\left[\begin{smallmatrix} 0 \\ 1/N \end{smallmatrix}\right]}(\tau) \\
&\iff \wp((z/N)\tau + w/N; [\tau, 1]) = \wp(1/N; [\tau, 1]) \\
&\qquad\qquad\qquad\qquad \text{by the definitions (2.1) and (2.2)} \\
&\iff (z/N)\tau + w/N \equiv \pm 1/N \pmod{[\tau, 1]} \quad \text{by lemma 2.1} \\
&\iff z \equiv 0,\ w \equiv \pm 1 \pmod{N}.
\end{aligned}$$

Thus we obtain

$$\mathrm{Gal}(\mathcal{F}_N/L) = \left\{\gamma \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) \;\middle|\; \gamma \equiv \pm \begin{bmatrix} * & * \\ 0 & 1 \end{bmatrix} \pmod{N}\right\}/\{\pm I_2\}, \tag{2.5}$$

and it follows from proposition 2.4, (F2) and (F3) that every element of $\mathrm{Gal}(\mathcal{F}_N/L)$ leaves

$$g_{\left[\begin{smallmatrix} 0 \\ 1/N \end{smallmatrix}\right]}(\tau)^{12N}$$

fixed. This implies that $\mathrm{Gal}(\mathcal{F}_N/L) \subseteq \mathrm{Gal}(\mathcal{F}_N/R)$.

Conversely, let $\rho = \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \in \mathrm{Gal}(\mathcal{F}_N/R)$. We then derive by proposition 2.4, (F2) and (F3) that

$$g_{\left[\begin{smallmatrix} c/N \\ d/N \end{smallmatrix}\right]}(\tau)^{12N} = g_{\left[\begin{smallmatrix} 0 \\ 1/N \end{smallmatrix}\right]}(\tau)^{12N}. \tag{2.6}$$

The action of $\left[\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right]$ on both sides of (2.6) yields

$$g_{\left[\begin{smallmatrix} d/N \\ -c/N \end{smallmatrix}\right]}(\tau)^{12N} = g_{\left[\begin{smallmatrix} 1/N \\ 0 \end{smallmatrix}\right]}(\tau)^{12N}. \tag{2.7}$$

By applying the q-order formula (2.4) to the expressions (2.6) and (2.7) we attain

$$6NB_2(\langle c/N \rangle) = 6NB_2(0) \quad \text{and} \quad 6NB_2(\langle d/N \rangle) = 6NB_2(1/N).$$

Now, we deduce by the shape of the graph $Y = B_2(X)$ that

$$c \equiv 0,\ d \equiv \pm 1 \pmod{N}.$$

This, together with (2.5), shows that $\mathrm{Gal}(\mathcal{F}_N/L) \supseteq \mathrm{Gal}(\mathcal{F}_N/R)$. Thus, we achieve $\mathrm{Gal}(\mathcal{F}_N/L) = \mathrm{Gal}(\mathcal{F}_N/R)$, and hence $L = R$, as desired.

(iii) For simplicity, let

$$f = f_{\left[\begin{smallmatrix} 0 \\ 1/N \end{smallmatrix}\right]}(\tau) \quad \text{and} \quad g = g_{\left[\begin{smallmatrix} 0 \\ 1/N \end{smallmatrix}\right]}(\tau)^{12N}.$$

By (i) we can express f as

$$f = c_0 + c_1 g + \cdots + c_{\ell-1} g^{\ell-1} \quad \text{for some } c_0, c_1, \ldots, c_{\ell-1} \in \mathcal{F}_1,$$

where $\ell = [\mathcal{F}_1(g) : \mathcal{F}_1]$. Multiplying both sides by g^k ($k = 0, 1, \ldots, \ell-1$) and taking traces $\mathrm{Tr} = \mathrm{Tr}_{\mathcal{F}_1(g)/\mathcal{F}_1}$ yields

$$\mathrm{Tr}(fg^k) = c_0 \,\mathrm{Tr}(g^k) + c_1 \,\mathrm{Tr}(g^{k+1}) + \cdots + c_{\ell-1} \,\mathrm{Tr}(g^{k+\ell-1}).$$

So we obtain a linear system (in unknowns $c_0, c_1, c_2, \ldots, c_{\ell-1}$)

$$T \begin{bmatrix} c_0 \\ c_1 \\ \vdots \\ c_{\ell-1} \end{bmatrix} = \begin{bmatrix} \mathrm{Tr}(f) \\ \mathrm{Tr}(fg) \\ \vdots \\ \mathrm{Tr}(fg^{\ell-1}) \end{bmatrix}, \quad \text{where } T = \begin{bmatrix} \mathrm{Tr}(1) & \mathrm{Tr}(g) & \cdots & \mathrm{Tr}(g^{\ell-1}) \\ \mathrm{Tr}(g) & \mathrm{Tr}(g^2) & \cdots & \mathrm{Tr}(g^{\ell}) \\ \vdots & \vdots & \ddots & \vdots \\ \mathrm{Tr}(g^{\ell-1}) & \mathrm{Tr}(g^{\ell}) & \cdots & \mathrm{Tr}(g^{2\ell-2}) \end{bmatrix}.$$

Since f and g are weakly holomorphic by (F1), so are all entries of the augmented matrix of the above linear system. Thus, we obtain by (i) that

$$c_0, c_1, \ldots, c_{\ell-1} \in (1/\det(T))\mathbb{Q}[j].$$

On the other hand, let $g_1, g_2, \ldots, g_\ell$ be all the zeros of $\min(g, \mathcal{F}_1)$. Then we see that

$$\begin{aligned} \det(T) &= \begin{vmatrix} \sum_{k=1}^{\ell} g_k^0 & \sum_{k=1}^{\ell} g_k^1 & \cdots & \sum_{k=1}^{\ell} g_k^{\ell-1} \\ \sum_{k=1}^{\ell} g_k^1 & \sum_{k=1}^{\ell} g_k^2 & \cdots & \sum_{k=1}^{\ell} g_k^{\ell} \\ \vdots & \vdots & \ddots & \vdots \\ \sum_{k=1}^{\ell} g_k^{\ell-1} & \sum_{k=1}^{\ell} g_k^{\ell} & \cdots & \sum_{k=1}^{\ell} g_k^{2\ell-2} \end{vmatrix} \\ &= \begin{vmatrix} g_1^0 & g_2^0 & \cdots & g_\ell^0 \\ g_1^1 & g_2^1 & \cdots & g_\ell^1 \\ \vdots & \vdots & \ddots & \vdots \\ g_1^{\ell-1} & g_2^{\ell-1} & \cdots & g_\ell^{\ell-1} \end{vmatrix} \begin{vmatrix} g_1^0 & g_1^1 & \cdots & g_1^{\ell-1} \\ g_2^0 & g_2^1 & \cdots & g_2^{\ell-1} \\ \vdots & \vdots & \ddots & \vdots \\ g_\ell^0 & g_\ell^1 & \cdots & g_\ell^{\ell-1} \end{vmatrix} \\ &= \prod_{1 \leqslant k_1 < k_2 \leqslant \ell} (g_{k_1} - g_{k_2})^2 \quad \text{by the Vandermonde determinant formula} \\ &= \mathrm{disc}(g, \mathcal{F}_1). \end{aligned}$$

This proves (iii). □

Remark 2.6. Define an equivalence relation $\sim$ on $\mathcal{V}_N$ as follows:

$$\boldsymbol{u} \sim \boldsymbol{v} \quad \text{if and only if} \quad \boldsymbol{u} \equiv \pm \boldsymbol{v} \pmod{\mathbb{Z}^2}.$$

Then, in a similar way as in the proof of lemma 2.5(ii), one can readily show that

$$f_{\boldsymbol{v}}(\tau) \text{ and } g_{\boldsymbol{v}}(\tau)^{12N} \text{ for } \boldsymbol{v} \in \mathcal{V}_N/\sim$$

represent all the distinct zeros of

$$\min\left(f_{\left[\begin{smallmatrix}0\\1/N\end{smallmatrix}\right]}(\tau), \mathcal{F}_1\right) \quad \text{and} \quad \min\left(g_{\left[\begin{smallmatrix}0\\1/N\end{smallmatrix}\right]}(\tau)^{12N}, \mathcal{F}_1\right),$$

respectively.

3. Generation of class fields

Let K be an imaginary quadratic field and let $\mathcal{O}_K$ be its ring of integers. Let $\mathfrak{n}$ be a proper non-trivial ideal of $\mathcal{O}_K$, let N (greater than or equal to 2) be the smallest positive integer in $\mathfrak{n}$ and let C be a ray class in the ray class group $\mathrm{Cl}(\mathfrak{n})$ of K modulo $\mathfrak{n}$. We take an integral ideal $\mathfrak{c}$ in the class C and let

$$\begin{aligned} \mathfrak{n}\mathfrak{c}^{-1} &= [\omega_1, \omega_2] \quad \text{for some } \omega_1, \omega_2 \in \mathbb{C} \text{ with } \omega = \omega_1/\omega_2 \in \mathbb{H}, \\ 1 &= (a/N)\omega_1 + (b/N)\omega_2 \quad \text{for some } a, b \in \mathbb{Z}. \end{aligned}$$

For a given Fricke family $\{h_{\boldsymbol{v}}(\tau)\}_{\boldsymbol{v}\in\mathcal{V}_N}$ of level N, we define the *Fricke invariant* $h_{\mathfrak{n}}(C)$ modulo $\mathfrak{n}$ at C by

$$h_{\mathfrak{n}}(C) = h_{\left[\begin{smallmatrix}a/N\\b/N\end{smallmatrix}\right]}(\omega). \tag{3.1}$$

This value depends only on $\mathfrak{n}$ and C, not on the choices of $\mathfrak{c}$, ω_1 and ω_2 [4, ch. 11, § 1].

PROPOSITION 3.1. *The Fricke invariant $h_{\mathfrak{n}}(C)$ lies in the ray class field $K_{\mathfrak{n}}$ of K modulo $\mathfrak{n}$ and satisfies the following transformation formula:*

$$h_{\mathfrak{n}}(C)^{\sigma_{\mathfrak{n}}(C')} = h_{\mathfrak{n}}(CC') \quad \textit{for any class } C' \in \mathrm{Cl}(\mathfrak{n}),$$

where $\sigma_{\mathfrak{n}}\colon \mathrm{Cl}(\mathfrak{n}) \to \mathrm{Gal}(K_{\mathfrak{n}}/K)$ is the Artin reciprocity map. Furthermore, the algebraic number $g_{\mathfrak{n}}^{12N}(C)/g_{\mathfrak{n}}^{12N}(C')$ is a unit.

Proof. See [4, ch. 11, theorems 1.1 and 1.2]. □

THEOREM 3.2. *Assume that K is different from $\mathbb{Q}(\sqrt{-1})$ and $\mathbb{Q}(\sqrt{-3})$. Then the first Fricke invariant $f_{\mathfrak{n}}(C)$ generates $K_{\mathfrak{n}}$ over the Hilbert class field H_K of K.*

Proof. Let C_0 be the identity class of $\mathrm{Cl}(\mathfrak{n})$. Since $K_{\mathfrak{n}}$ is a finite abelian extension of K, it suffices to show that $f_{\mathfrak{n}}(C_0)$ generates $K_{\mathfrak{n}}$ over H_K. Let

$$\begin{aligned} I_K(\mathfrak{n}) &= \text{the group of fractional ideals of } K \text{ prime to } \mathfrak{n}, \\ P_K(\mathfrak{n}) &= \langle \alpha\mathcal{O}_K \mid \alpha \in \mathcal{O}_K \text{ such that } \alpha\mathcal{O}_K \text{ is prime to } \mathfrak{n} \rangle \quad (\subseteq I_K(\mathfrak{n})), \\ P_{K,1}(\mathfrak{n}) &= \langle \alpha\mathcal{O}_K \mid \alpha \in \mathcal{O}_K \text{ such that } \alpha \equiv 1 \pmod{\mathfrak{n}} \rangle \quad (\subseteq P_K(\mathfrak{n})). \end{aligned}$$

Since $\mathrm{Gal}(K_{\mathfrak{n}}/K) \simeq I_K(\mathfrak{n})/P_{K,1}(\mathfrak{n})$ and $\mathrm{Gal}(H_K/K) \simeq I_K(\mathfrak{n})/P_K(\mathfrak{n})$ [3, ch. IV and V], we get

$$\mathrm{Gal}(K_{\mathfrak{n}}/H_K) \simeq P_K(\mathfrak{n})/P_{K,1}(\mathfrak{n}). \tag{3.2}$$

Assume that a class D in $P_K(\mathfrak{n})/P_{K,1}(\mathfrak{n})$ leaves $f_{\mathfrak{n}}(C_0)$ fixed via the Artin reciprocity law. Here we may assume that $D = [\alpha\mathcal{O}_K]$ for some $\alpha \in \mathcal{O}_K$ such that

$\alpha\mathcal{O}_K$ is prime to $\mathfrak{n}$, since $P_K(\mathfrak{n})/P_{K,1}(\mathfrak{n})$ is a finite group. Take $\mathfrak{c} = \mathcal{O}_K \in C_0$ and let

$$\mathfrak{n}\mathfrak{c}^{-1} = \mathfrak{n} = [\omega_1, \omega_2] \quad \text{for some } \omega_1, \omega_2 \in \mathbb{C} \text{ with } \omega = \omega_1/\omega_2 \in \mathbb{H}, \tag{3.3}$$

$$1 = (a/N)\omega_1 + (b/N)\omega_2 \quad \text{for some } a, b \in \mathbb{Z}. \tag{3.4}$$

We then have

$$\mathfrak{n}(\alpha\mathcal{O}_K)^{-1} = [\omega_1\alpha^{-1}, \omega_2\alpha^{-1}], \tag{3.5}$$

$$1 = (r/N)(\omega_1\alpha^{-1}) + (s/N)(\omega_2\alpha^{-1}) \quad \text{for some } r, s \in \mathbb{Z}. \tag{3.6}$$

Now we attain that

$$\begin{aligned} f_{\mathfrak{n}}(C_0) &= f_{\left[\begin{smallmatrix} a/N \\ b/N \end{smallmatrix}\right]}(\omega) \quad \text{by (3.3), (3.4) and definition (3.1)} \\ &= f_{\mathfrak{n}}(C_0)^{\sigma_{\mathfrak{n}}(D)} \\ &= f_{\mathfrak{n}}(D) \quad \text{by proposition 3.1 and the fact that } C_0 \text{ is} \\ &\qquad\qquad\qquad\qquad\qquad\qquad \text{the identity class of } \mathrm{Cl}(\mathfrak{n}) \\ &= f_{\left[\begin{smallmatrix} r/N \\ s/N \end{smallmatrix}\right]}(\omega_1\alpha^{-1}/\omega_2\alpha^{-1}) \quad \text{by (3.5), (3.6) and definition (3.1)} \\ &= f_{\left[\begin{smallmatrix} r/N \\ s/N \end{smallmatrix}\right]}(\omega). \end{aligned}$$

Note that since K is different from $\mathbb{Q}(\sqrt{-1})$ and $\mathbb{Q}(\sqrt{-3})$, we get $g_2(\omega), g_3(\omega) \neq 0$ [5, ch. 3, theorem 3]. We thus obtain by definition (2.2) and lemma 2.1 that

$$(a/N)\omega + b/N \equiv \pm((r/N)\omega + s/N) \pmod{[\omega, 1]}.$$

It then follows that

$$(a/N)\omega_1 + (b/N)\omega_2 \equiv \pm((r/N)\omega_1 + (s/N)\omega_2) \pmod{[\omega_1, \omega_2]},$$

and hence

$$1 \equiv \pm\alpha \pmod{\mathfrak{n}}$$

by (3.3), (3.4) and (3.6). This shows that the class $D = [\alpha\mathcal{O}_K]$ gives rise to the identity of $\mathrm{Gal}(K_{\mathfrak{n}}/H_K)$ via the Artin reciprocity map by (3.2). Therefore, we conclude by Galois theory that $f_{\mathfrak{n}}(C_0)$ generates $K_{\mathfrak{n}}$ over H_K. □

4. Siegel–Ramachandra invariants

Let K be an imaginary quadratic field other than $\mathbb{Q}(\sqrt{-1})$ and $\mathbb{Q}(\sqrt{-3})$. Let d_K be its discriminant and set

$$\tau_K = \begin{cases} (-1 + \sqrt{d}_K)/2 & \text{if } d_K \equiv 1 \pmod 4, \\ \sqrt{d_K}/2 & \text{if } d_K \equiv 0 \pmod 4) \end{cases}$$

so that $\tau_K \in \mathbb{H}$ and $\mathcal{O}_K = [\tau_K, 1]$. Then, as is well known, the special value $j(\tau_K)$ generates H_K over K [5, ch. 10, theorem 1]. Let $\mathfrak{n}$ be a proper non-trivial ideal of $\mathcal{O}_K$, let N (greater than or equal to 2) be the smallest positive integer in $\mathfrak{n}$ and let

https://doi.org/10.1017/S0308210515000608 Published online by Cambridge University Press

$C \in \mathrm{Cl}(\mathfrak{n})$. We call the Fricke invariant $g_{\mathfrak{n}}^{12N}(C)$ the *Siegel–Ramachandra invariant* modulo $\mathfrak{n}$ at C [6]. We furthermore let

$$d_N(\tau) = \mathrm{disc}\Big(g_{\left[\begin{smallmatrix}0\\1/N\end{smallmatrix}\right]}(\tau)^{12N}, \mathcal{F}_1\Big).$$

THEOREM 4.1. *If the special value $d_N(\tau_K)$ is non-zero, then $g_{\mathfrak{n}}^{12N}(C)$ generates $K_{\mathfrak{n}}$ over H_K.*

Proof. As in the proof of theorem 3.2 we let $C = C_0$ (the identity class of $\mathrm{Cl}(\mathfrak{n})$) and let

$$f_{\mathfrak{n}}(C_0) = f_{\left[\begin{smallmatrix}a/N\\b/N\end{smallmatrix}\right]}(\omega) \quad \text{and} \quad g_{\mathfrak{n}}^{12N}(C_0) = g_{\left[\begin{smallmatrix}a/N\\b/N\end{smallmatrix}\right]}(\omega)^{12N}$$
$$\text{for some } \begin{bmatrix}a/N\\b/N\end{bmatrix} \in \mathcal{V}_N \text{ and } \omega \in \mathbb{H}.$$

Since $d_N(\tau)$ is weakly holomorphic by remark 2.6, proposition 2.4 and (F1), we get by lemma 2.5(i) that

$$d_N(\tau) = d(j(\tau)) \quad \text{for some polynomial } d(X) \in \mathbb{Q}[X]. \tag{4.1}$$

We then have $d_N(\tau_K) = d(j(\tau_K)) \neq 0$ by assumption, and hence $d(j(\omega)) \neq 0$ because $j(\omega)$ is a Galois conjugate of $j(\tau_K)$ over K [5, ch. 10, theorem 1].

Now, take an element $\gamma \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I_2\} \simeq \mathrm{Gal}(\mathcal{F}_N/\mathcal{F}_1)$ such that $\gamma \equiv \pm\left[\begin{smallmatrix}* & *\\ a & b\end{smallmatrix}\right] \pmod N$. We then derive that

$$\begin{aligned}
f_{\mathfrak{n}}(C_0) &= f_{\left[\begin{smallmatrix}a/N\\b/N\end{smallmatrix}\right]}(\omega)\\
&= f_{{}^{\mathrm{t}}\gamma\left[\begin{smallmatrix}0\\1/N\end{smallmatrix}\right]}(\omega) \quad \text{by proposition 2.2 and (F2)}\\
&= \Big(f_{\left[\begin{smallmatrix}0\\1/N\end{smallmatrix}\right]}(\tau)\Big)^{\gamma}(\omega) \quad \text{by (F3)}\\
&= \Big(p\Big(j(\tau), g_{\left[\begin{smallmatrix}0\\1/N\end{smallmatrix}\right]}(\tau)^{12N}\Big)/d(j(\tau))\Big)^{\gamma}(\omega)\\
&\qquad\qquad \text{for some polynomial } p(X,Y) \in \mathbb{Q}[X,Y] \text{ by lemma 2.5(iii)}\\
&= \Big(p\Big(j(\tau), \Big(g_{\left[\begin{smallmatrix}0\\1/N\end{smallmatrix}\right]}(\tau)^{12N}\Big)^{\gamma}\Big)/d(j(\tau))\Big)(\omega) \quad \text{because } \gamma \text{ fixes } j(\tau) \in \mathcal{F}_1\\
&= \Big(p\Big(j(\tau), \Big(g_{{}^{\mathrm{t}}\gamma\left[\begin{smallmatrix}0\\1/N\end{smallmatrix}\right]}(\tau)^{12N}\Big)\Big)/d(j(\tau))\Big)(\omega)\\
&\qquad\qquad \text{by proposition 2.4, (F2) and (F3)}\\
&= \Big(p\Big(j(\tau), g_{\left[\begin{smallmatrix}a/N\\b/N\end{smallmatrix}\right]}(\tau)^{12N}\Big)/d(j(\tau))\Big)(\omega)\\
&= p(j(\omega), g_{\mathfrak{n}}^{12N}(C_0))/d(j(\omega)).
\end{aligned}$$

Thus we achieve that

$$\begin{aligned} K_{\mathfrak{n}} &= H_K(f_{\mathfrak{n}}(C_0)) \quad \text{by theorem 3.2} \\ &= H_K(p(j(\omega), g_{\mathfrak{n}}^{12N}(C_0))/d(j(\omega))) \\ &\subseteq H_K(j(\omega), g_{\mathfrak{n}}^{12N}(C_0)) \quad \text{since } d(j(\omega)) \neq 0 \\ &= H_K(g_{\mathfrak{n}}^{12N}(C_0)) \quad \text{because } H_K = K(j(\omega)) \\ &\subseteq K_{\mathfrak{n}} \quad \text{by proposition 3.1.} \end{aligned}$$

This proves that $K_{\mathfrak{n}} = H_K(g_{\mathfrak{n}}^{12N}(C_0))$, as desired. □

REMARK 4.2. Here, we conjecture that $d_N(\tau_K) \neq 0$ for all integers $N \geqslant 2$ and all imaginary quadratic fields K other than $\mathbb{Q}(\sqrt{-1})$ and $\mathbb{Q}(\sqrt{-3})$.

COROLLARY 4.3. *Let h_K be the class number of K and*

$$\ell_N = \Big[\mathcal{F}_1\Big(g_{\left[\begin{smallmatrix}0\\1/N\end{smallmatrix}\right]}(\tau)^{12N}\Big) : \mathcal{F}_1\Big].$$

If $h_K > N\ell_N(\ell_N - 1)/2$, then $g_{\mathfrak{n}}^{12N}(C)$ generates $K_{\mathfrak{n}}$ over H_K.

Proof. Letting $g_1, g_2, \ldots, g_{\ell_N}$ be all the zeros of the polynomial

$$\min\Big(g_{\left[\begin{smallmatrix}0\\1/N\end{smallmatrix}\right]}(\tau)^{12N}, \mathcal{F}_1\Big) \in \mathcal{F}_1[X]$$

we see that

$$\begin{aligned} \mathrm{ord}_q(d_N(\tau)) &= \mathrm{ord}_q\Bigg(\prod_{1\leqslant k_1<k_2\leqslant \ell_N}(g_{k_1} - g_{k_2})^2\Bigg) \\ &= 2\sum_{1\leqslant k_1<k_2\leqslant \ell_N} \mathrm{ord}_q(g_{k_1} - g_{k_2}) \\ &\geqslant 2\sum_{1\leqslant k_1<k_2\leqslant \ell_N} \min\{\mathrm{ord}_q(g_{k_1}), \mathrm{ord}_q(g_{k_2})\} \\ &\geqslant 2\sum_{1\leqslant k_1<k_2\leqslant \ell_N} 6NB_2(1/2) \\ &\qquad \text{by remark 2.6, (2.4) and the shape of the graph } Y = B_2(X) \\ &= -N\ell_N(\ell_N - 1)/2. \end{aligned}$$

Let $d(X)$ be the polynomial in $\mathbb{Q}[X]$ given in (4.1). Since $\mathrm{ord}_q(j(\tau)) = -1$, we obtain

$$\deg(d(X)) \leqslant N\ell_N(\ell_N - 1)/2.$$

Now, the assumption $h_K = \deg(\min(j(\tau_K), K)) > N\ell_N(\ell_N - 1)/2$ implies that

$$d_N(\tau_K) = d(j(\tau_K)) \neq 0.$$

Thus, the result follows from theorem 4.1. □

https://doi.org/10.1017/S0308210515000608 Published online by Cambridge University Press

5. Shimura's reciprocity law

Let K be an imaginary quadratic field other than $\mathbb{Q}(\sqrt{-1})$ and $\mathbb{Q}(\sqrt{-3})$. For a positive integer N let $\mathfrak{n} = N\mathcal{O}_K$ and let

$$\mathcal{F}_{N,K} = \{h(\tau) \in \mathcal{F}_N \mid h(\tau) \text{ is finite at } \tau_K\}.$$

As a consequence of the theory of complex multiplication we obtain the following proposition.

PROPOSITION 5.1. *We have* $K_{\mathfrak{n}} = K(h(\tau_K) \mid h(\tau) \in \mathcal{F}_{N,K})$.

Proof. See [5, ch. 10, corollary to theorem 2]. □

PROPOSITION 5.2 (Shimura's reciprocity law). *Let* $\min(\tau_K, \mathbb{Q}) = X^2 + bX + c \in \mathbb{Z}[X]$. *The matrix group*

$$\mathcal{W}_{N,K} = \left\{ \begin{bmatrix} t - bs & -cs \\ s & t \end{bmatrix} \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) \;\middle|\; t, s \in \mathbb{Z}/N\mathbb{Z} \right\}$$

gives rise to the isomorphism

$$\begin{aligned} &\mathcal{W}_{N,K}/\{\pm I_2\} \to \mathrm{Gal}(K_{\mathfrak{n}}/H_K) \\ &\qquad \alpha \mapsto h(\tau_K) \mapsto h(\tau)^{\alpha}(\tau_K), \quad h(\tau) \in \mathcal{F}_{N,K}. \end{aligned}$$

Proof. See [11, § 3]. □

REMARK 5.3. Let $x = s\tau_K + t \in \mathcal{O}_K$ with $s, t \in \mathbb{Z}$. If $x\mathcal{O}_K$ is relatively prime to $\mathfrak{n}$, then the class $[x\mathcal{O}_K]$ in $P_K(\mathfrak{n})/P_{K,1}(\mathfrak{n})$ corresponds to the matrix

$$\begin{bmatrix} t - bs & -cs \\ s & t \end{bmatrix} \in \mathcal{W}_{N,K}/\{\pm I_2\};$$

see [5, ch. 11, § 1] and [11].

LEMMA 5.4. *Assume that* $N \equiv 0 \pmod 4$. *We have*

$$g_{\left[\begin{smallmatrix} 1/2 \\ 1/2+1/N \end{smallmatrix}\right]}(\tau_K)^{12N} / g_{\left[\begin{smallmatrix} 0 \\ 1/N \end{smallmatrix}\right]}(\tau_K)^{12N} = g_{\mathfrak{n}}^{12N}(C)/g_{\mathfrak{n}}^{12N}(C_0),$$

where $C = [((N/2)\tau_K + N/2 + 1)\mathcal{O}_K]$, $C_0 = [\mathcal{O}_K] \in \mathrm{Cl}(\mathfrak{n})$. *This value is a unit in* $K_{\mathfrak{n}}$.

Proof. If we take $\mathfrak{c} = \mathcal{O}_K \in C_0$, then we have

$$\mathfrak{n}\mathfrak{c}^{-1} = \mathfrak{n} = [N\tau_K, N] \quad \text{and} \quad 1 = 0(N\tau_K) + (1/N)N.$$

So we get by definition (3.1),

$$g_{\mathfrak{n}}^{12N}(C_0) = g_{\left[\begin{smallmatrix} 0 \\ 1/N \end{smallmatrix}\right]}(\tau_K)^{12N}. \tag{5.1}$$

By remark 5.3, the class $C = [((N/2)\tau_K + N/2 + 1)\mathcal{O}_K] \in P_K(\mathfrak{n})/P_{K,1}(\mathfrak{n})$ corresponds to

$$\alpha = \begin{cases} \begin{bmatrix} 1 & ((1-d_K)/4)(N/2) \\ N/2 & N/2+1 \end{bmatrix} & \text{if } d_K \equiv 1 \pmod 4, \\ \begin{bmatrix} N/2+1 & (d_K/4)(N/2) \\ N/2 & N/2+1 \end{bmatrix} & \text{if } d_K \equiv 0 \pmod 4 \end{cases}$$

in $\mathcal{W}_{N,K}/\{\pm I_2\}$. We then deduce that

$$\begin{aligned} g_{\mathfrak{n}}^{12N}(C)/g_{\mathfrak{n}}^{12N}(C_0) &= g_{\mathfrak{n}}^{12N}(C_0)^{\sigma_{\mathfrak{n}}(C)}/g_{\mathfrak{n}}^{12N}(C_0) \quad \text{by proposition 3.1} \\ &= \Bigl(g_{\left[\begin{smallmatrix} 0 \\ 1/N \end{smallmatrix}\right]}(\tau_K)^{12N}\Bigr)^{\sigma_{\mathfrak{n}}(C)} / g_{\left[\begin{smallmatrix} 0 \\ 1/N \end{smallmatrix}\right]}(\tau_K)^{12N} \quad \text{by (5.1)} \\ &= \Bigl(g_{\left[\begin{smallmatrix} 0 \\ 1/N \end{smallmatrix}\right]}(\tau)^{12N}\Bigr)^{\alpha}(\tau_K) / g_{\left[\begin{smallmatrix} 0 \\ 1/N \end{smallmatrix}\right]}(\tau_K)^{12N} \quad \text{by proposition 5.2} \\ &= g_{{}^{t}\alpha\left[\begin{smallmatrix} 0 \\ 1/N \end{smallmatrix}\right]}(\tau)^{12N}(\tau_K) / g_{\left[\begin{smallmatrix} 0 \\ 1/N \end{smallmatrix}\right]}(\tau_K)^{12N} \\ &\qquad\qquad \text{by proposition 2.4, (F2) and (F3)} \\ &= g_{\left[\begin{smallmatrix} 1/2 \\ 1/2+1/N \end{smallmatrix}\right]}(\tau_K)^{12N} / g_{\left[\begin{smallmatrix} 0 \\ 1/N \end{smallmatrix}\right]}(\tau_K)^{12N}. \end{aligned}$$

And this is a unit in $K_{\mathfrak{n}}$ by proposition 3.1. □

6. Invariants with small exponents

Let K be an imaginary quadratic field of discriminant d_K. For a positive integer N let $\mathfrak{n} = N\mathcal{O}_K$. Throughout this section we assume that

(i) $N \geqslant 4$ and $N \equiv 0 \pmod 2$,

(ii) $|d_K| \geqslant 4N^{4/3}$ (greater than 25) and $d_K \equiv 0 \pmod 4$.

Lemma 6.1. *Let* $\boldsymbol{v} = \left[\begin{smallmatrix} a/N \\ b/N \end{smallmatrix}\right] \in \mathcal{V}_N$.

(i) *If* $\boldsymbol{v} \not\equiv \pm\left[\begin{smallmatrix} 0 \\ 1/N \end{smallmatrix}\right] \pmod{\mathbb{Z}^2}$, *then we have*

$$|g_{\boldsymbol{v}}(\tau_K)| > \Bigl|g_{\left[\begin{smallmatrix} 0 \\ 1/N \end{smallmatrix}\right]}(\tau_K)\Bigr|.$$

(ii) *We also get*

$$|g_{\boldsymbol{v}}(\tau_K)| \leqslant \Bigl|g_{\left[\begin{smallmatrix} 1/2 \\ 1/2+1/N \end{smallmatrix}\right]}(\tau_K)\Bigr|.$$

Proof. Since $g_{\boldsymbol{v}}(\tau)^{12N}$ depends only on $\pm\boldsymbol{v} \pmod{\mathbb{Z}^2}$ by proposition 2.4 and (F2), we may assume that $0 \leqslant a/N \leqslant 1/2$ and $0 \leqslant b/N < 1$. Now that $d_K \equiv 0 \pmod 4$, we have $\tau_K = \sqrt{d_K}/2$. We then obtain by (2.3) that

$$\begin{aligned}|g_{\boldsymbol{v}}(\tau_K)|^2 = A^{B_2(a/N)}(1 - 2\cos(2\pi b/N)A^{a/N} + A^{2a/N})\\ \times \prod_{n=1}^{\infty}\{(1 - 2\cos(2\pi b/N)A^{n+a/N} + A^{2(n+a/N)})\\ \times (1 - 2\cos(2\pi b/N)A^{n-a/N} + A^{2(n-a/N)})\},\end{aligned} \tag{6.1}$$

where $A = \mathrm{e}^{-\pi\sqrt{|d_K|}}$ (less than $\mathrm{e}^{-5\pi}$).

(i) If $a/N = 0$, then the assumption $\boldsymbol{v} \not\equiv \pm\left[\begin{smallmatrix}0\\1/N\end{smallmatrix}\right] \pmod{\mathbb{Z}^2}$ yields $2/N \leqslant b/N \leqslant (N-2)/N$. Hence, we obtain by (6.1) and the shape of the graph $Y = \cos X$ that

$$|g_{\boldsymbol{v}}(\tau_K)| > \left|g_{\left[\begin{smallmatrix}0\\1/N\end{smallmatrix}\right]}(\tau_K)\right|.$$

Now, let $1/N \leqslant a/N \leqslant 1/2$. We see by (6.1) and the shape of the graph $Y = B_2(X)$ that

$$|g_{\boldsymbol{v}}(\tau_K)| \geqslant \left|g_{\left[\begin{smallmatrix}a/N\\0\end{smallmatrix}\right]}(\tau_K)\right|. \tag{6.2}$$

Furthermore, we derive by (6.1) that

$$\begin{aligned}&\left|g_{\left[\begin{smallmatrix}0\\1/N\end{smallmatrix}\right]}(\tau_K)\right| \Big/ \left|g_{\left[\begin{smallmatrix}a/N\\0\end{smallmatrix}\right]}(\tau_K)\right|\\
&\leqslant \frac{A^{\frac{1}{2}B_2(0)}2\sin(\pi/N)\prod_{n=1}^{\infty}(1+A^{2n})}{A^{\frac{1}{2}B_2(a/N)}(1-A^{a/N})\prod_{n=1}^{\infty}(1-A^{n+a/N})(1-A^{n-a/N})}\\
&\qquad\qquad\text{because } \cos(2\pi/N) \geqslant 0 \text{ for } N \geqslant 4\\
&\leqslant \frac{2\sin(\pi/N)A^{\frac{1}{2}B_2(0)}\prod_{n=1}^{\infty}(1+A^{n/4})}{A^{\frac{1}{2}B_2(1/N)}(1-A^{1/N})\prod_{n=1}^{\infty}(1-A^{n/2})^2}\\
&\qquad\text{by the shape of the graph } Y = B_2(X) \text{ and the fact that } 1/N \leqslant a/N \leqslant 1/2\\
&\leqslant \frac{2\sin(\pi/N)A^{\frac{1}{2}(B_2(0)-B_2(1/N))}}{(1-A^{1/N})}\prod_{n=1}^{\infty}(1+A^{n/4})^3\\
&\qquad\qquad\text{by the inequality } (1-A^{n/2})(1+A^{n/4}) > 1 \text{ due to } A < \mathrm{e}^{-5\pi}\\
&\leqslant \frac{2\sin(\pi/N)A^{(1/2N)(1-1/N)}}{(1-A^{1/N})}\exp\left\{\sum_{n=1}^{\infty}3A^{n/4}\right\}\\
&\qquad\qquad\text{by the fact } 1+X < \mathrm{e}^X \text{ for } X > 0\\
&\leqslant \frac{2\sin(\pi/N)\mathrm{e}^{-\pi N^{-1/3}(1-1/N)}}{(1-\mathrm{e}^{-2\pi N^{-1/3}})}\mathrm{e}^{3A^{1/4}/(1-A^{1/4})} \quad \text{by the assumption } |d_K| \geqslant 4N^{4/3}\end{aligned}$$

https://doi.org/10.1017/S0308210515000608 Published online by Cambridge University Press

$$< 0.4\mathrm{e}^{3\mathrm{e}^{-5\pi/4}/(1-\mathrm{e}^{-5\pi/4})}$$

by considering the graph of $Y = \dfrac{2\sin(\pi/X)\mathrm{e}^{-\pi X^{-1/3}(1-1/X)}}{(1-\mathrm{e}^{-2\pi X^{-1/3}})}$ at $X \geqslant 4$ and the fact that $A < \mathrm{e}^{-5\pi}$

$$< 1.$$

Thus, we attain by (6.2),

$$|g_{\boldsymbol{v}}(\tau_K)| > \left|g_{\left[\begin{smallmatrix}0\\1/N\end{smallmatrix}\right]}(\tau_K)\right|.$$

(ii) Considering the shape of the graphs $Y = B_2(X)$ and $Y = \cos X$ and the fact that $\boldsymbol{v} \in \mathcal{V}_N$, we deduce that

$$|g_{\boldsymbol{v}}(\tau_K)| \leqslant \max\left\{\left|g_{\left[\begin{smallmatrix}1/2-1/N\\1/2\end{smallmatrix}\right]}(\tau_K)\right|, \left|g_{\left[\begin{smallmatrix}1/2\\1/2+1/N\end{smallmatrix}\right]}(\tau_K)\right|\right\}.$$

So it suffices to show that

$$\left|g_{\left[\begin{smallmatrix}1/2-1/N\\1/2\end{smallmatrix}\right]}(\tau_K)\right| \leqslant \left|g_{\left[\begin{smallmatrix}1/2\\1/2+1/N\end{smallmatrix}\right]}(\tau_K)\right|$$

in order to prove that

$$|g_{\boldsymbol{v}}(\tau_K)| \leqslant \left|g_{\left[\begin{smallmatrix}1/2\\1/2+1/N\end{smallmatrix}\right]}(\tau_K)\right|.$$

Now we derive that

$$\begin{aligned}
&\left|g_{\left[\begin{smallmatrix}1/2-1/N\\1/2\end{smallmatrix}\right]}(\tau_K)\right| \Big/ \left|g_{\left[\begin{smallmatrix}1/2\\1/2+1/N\end{smallmatrix}\right]}(\tau_K)\right| \\
&\quad \leqslant \frac{A^{\frac{1}{2}B_2(1/2-1/N)}(1+A^{1/2-1/N})\prod_{n=1}^{\infty}(1+A^{n+1/2-1/N})(1+A^{n-1/2+1/N})}{A^{\frac{1}{2}B_2(1/2)}} \\
&\qquad\qquad \text{by (6.1) and the fact that } \cos(2\pi/N) \geqslant 0 \text{ for } N \geqslant 4 \\
&\quad \leqslant A^{1/2N^2}(1+A^{1/4})\prod_{n=1}^{\infty}(1+A^{n+1/4})(1+A^{n-1/2}) \quad \text{because } N \geqslant 4 \\
&\quad \leqslant A^{1/2N^2}\prod_{n=1}^{\infty}(1+A^{n/4}) \\
&\quad \leqslant A^{1/2N^2}\exp\left\{\sum_{n=1}^{\infty}A^{n/4}\right\} \quad \text{due to the fact } 1+X < \mathrm{e}^X \text{ for all } X > 0 \\
&\quad \leqslant \mathrm{e}^{-\pi/N^{4/3}}\exp\left\{\sum_{n=1}^{\infty}\mathrm{e}^{-(\pi N^{2/3}/2)n}\right\} \quad \text{since } |d_K| \geqslant 4N^{4/3} \\
&\quad = \exp\{-\pi/N^{4/3} + \mathrm{e}^{-\pi N^{2/3}/2}/(1-\mathrm{e}^{-\pi N^{2/3}/2})\} \\
&\quad < \exp\{-\pi/N^{4/3} + 8/\pi^2 N^{4/3}(1-\mathrm{e}^{-\pi N^{2/3}/2})\} \\
&\qquad\qquad \text{because } \mathrm{e}^{-X} < 2X^{-2} \text{ for all } X > 0
\end{aligned}$$

https://doi.org/10.1017/S0308210515000608 Published online by Cambridge University Press

$$
\begin{aligned}
&= \exp\{(\pi/N^{4/3})(-1 + 8/\pi^3(1 - \mathrm{e}^{-\pi N^{2/3}/2}))\} \\
&\leqslant \exp\{(\pi/N^{4/3})(-1 + 8/\pi^3(1 - \mathrm{e}^{-\pi 2^{1/3}}))\} \quad \text{owing to the fact } N \geqslant 4 \\
&< 1.
\end{aligned}
$$

This proves (ii). □

THEOREM 6.2. *The special value*

$$
\zeta_{2N}^{-4/\gcd(4,N)}\Big(g_{\left[\begin{smallmatrix}1/2\\1/2+1/N\end{smallmatrix}\right]}(\tau_K)/g_{\left[\begin{smallmatrix}0\\1/N\end{smallmatrix}\right]}(\tau_K)\Big)^{8/\gcd(4,N)} \tag{6.3}
$$

generates $K_{\mathfrak{n}}$ *over* H_K*. Moreover, if* $N \equiv 0 \pmod 4$*, then it is a* $6N$*th root of the unit* $g_{\mathfrak{n}}^{12N}(C)/g_{\mathfrak{n}}^{12N}(C_0)$*, where* $C = [((N/2)\tau_K + N/2 + 1)\mathcal{O}_K]$ *and* $C_0 = [\mathcal{O}_K]$*.*

Proof. Since

$$
\zeta_{2N}^{-4/\gcd(4,N)}\Big(g_{\left[\begin{smallmatrix}1/2\\1/2+1/N\end{smallmatrix}\right]}(\tau)/g_{\left[\begin{smallmatrix}0\\1/N\end{smallmatrix}\right]}(\tau)\Big)^{8/\gcd(4,N)}
$$

belongs to $\mathcal{F}_N$ by lemma 2.3, its special value at τ_K lies in $K_{\mathfrak{n}}$ by proposition 5.1. Let $\sigma \in \mathrm{Gal}(K_{\mathfrak{n}}/H_K)$ such that $\sigma \neq \mathrm{id}$. We observe that

$$
\begin{aligned}
\left|\left(\frac{g_{\left[\begin{smallmatrix}1/2\\1/2+1/N\end{smallmatrix}\right]}(\tau_K)^{12N}}{g_{\left[\begin{smallmatrix}0\\1/N\end{smallmatrix}\right]}(\tau_K)^{12N}}\right)^{\sigma}\right|
&= \left|\frac{\Big(g_{\left[\begin{smallmatrix}1/2\\1/2+1/N\end{smallmatrix}\right]}(\tau_K)^{12N}\Big)^{\sigma}}{\Big(g_{\left[\begin{smallmatrix}0\\1/N\end{smallmatrix}\right]}(\tau_K)^{12N}\Big)^{\sigma}}\right| \\
&\qquad \text{by lemma 2.3 and proposition 5.1} \\
&= \left|\frac{\Big(g_{\left[\begin{smallmatrix}1/2\\1/2+1/N\end{smallmatrix}\right]}(\tau)^{12N}\Big)^{\alpha}(\tau_K)}{\Big(g_{\left[\begin{smallmatrix}0\\1/N\end{smallmatrix}\right]}(\tau)^{12N}\Big)^{\alpha}(\tau_K)}\right| \\
&\qquad \text{for some } \alpha \in \mathcal{W}_{N,K}/\{\pm I_2\} \text{ by proposition 5.2} \\
&= \left|\frac{g_{\boldsymbol{u}}(\tau_K)^{12N}}{g_{\boldsymbol{v}}(\tau_K)^{12N}}\right| \quad \text{for some } \boldsymbol{u}, \boldsymbol{v} \in \mathcal{V}_N \\
&\qquad \text{by proposition 2.4, (F2) and (F3)} \\
&< \left|\frac{g_{\left[\begin{smallmatrix}1/2\\1/2+1/N\end{smallmatrix}\right]}(\tau_K)^{12N}}{g_{\left[\begin{smallmatrix}0\\1/N\end{smallmatrix}\right]}(\tau_K)^{12N}}\right| \quad \text{by lemma 6.1.}
\end{aligned}
$$

This implies that the value in (6.3) generates $K_{\mathfrak{n}}$ over H_K. The second part of the theorem follows from lemma 5.4. □

Remark 6.3.

(i) Theorem 6.2 deals with a special case of [8, conjecture 6.8.3].

(ii) Suppose that N is not a power of 2, and so N has at least two prime factors. Then both $g_{\boldsymbol{v}}(\tau)^{12N}$ and $g_{\boldsymbol{v}}(\tau)^{-12N}$ are integral over $\mathbb{Z}[j(\tau)]$ for any $\boldsymbol{v} \in \mathcal{V}_N$ [4, ch. 2, theorem 2.2]. Moreover, since $j(\tau_K)$ is an algebraic integer [9, theorem 4.14], we see that $g_{\boldsymbol{v}}(\tau_K)^{12N}$ is a unit. Therefore, the invariant in (6.3) is a unit.

(iii) For any $\boldsymbol{u}, \boldsymbol{v} \in \mathbb{Q}^2 \setminus \mathbb{Z}^2$ such that $\boldsymbol{u} \not\equiv \pm\boldsymbol{v} \pmod{\mathbb{Z}^2}$ we have the relation

$$\wp_{\boldsymbol{u}}(\tau) - \wp_{\boldsymbol{v}}(\tau) = -(g_{\boldsymbol{u}+\boldsymbol{v}}(\tau) g_{\boldsymbol{u}-\boldsymbol{v}}(\tau)/g_{\boldsymbol{u}}(\tau)^2 g_{\boldsymbol{v}}(\tau)^2)\eta(\tau)^4;$$

see [4, p. 51]. This relation together with (2.2) and (2.3) yields

$$\frac{f_{\left[\begin{smallmatrix}0\\1/N\end{smallmatrix}\right]}(\tau_K) - f_{\left[\begin{smallmatrix}1/2\\1/2\end{smallmatrix}\right]}(\tau_K)}{f_{\left[\begin{smallmatrix}0\\1/2\end{smallmatrix}\right]}(\tau_K) - f_{\left[\begin{smallmatrix}1/2\\1/2\end{smallmatrix}\right]}(\tau_K)} = -\zeta_{2N} \frac{g_{\left[\begin{smallmatrix}1/2\\1/2+1/N\end{smallmatrix}\right]}(\tau_K)^2}{g_{\left[\begin{smallmatrix}0\\1/N\end{smallmatrix}\right]}(\tau_K)^2} \zeta_4^3 \frac{g_{\left[\begin{smallmatrix}0\\1/2\end{smallmatrix}\right]}(\tau_K)^2}{g_{\left[\begin{smallmatrix}1/2\\0\end{smallmatrix}\right]}(\tau_K)^2}. \tag{6.4}$$

Since

$$f_{\mathfrak{n}}(C_0) = f_{\left[\begin{smallmatrix}0\\1/N\end{smallmatrix}\right]}(\tau_K)$$

generates $K_{\mathfrak{n}}$ over H_K by theorem 3.2, and

$$f_{\left[\begin{smallmatrix}1/2\\1/2\end{smallmatrix}\right]}(\tau_K) \quad \text{and} \quad f_{\left[\begin{smallmatrix}0\\1/2\end{smallmatrix}\right]}(\tau_K)$$

lie in $K_{2\mathcal{O}_K}$ by propositions 2.2 and 5.1, the value in the left-hand side of (6.4) generates $K_{\mathfrak{n}}$ over $K_{2\mathcal{O}_K}$. Now, assume that $N \equiv 0 \pmod 4$. Since

$$\zeta_4^3 g_{\left[\begin{smallmatrix}0\\1/2\end{smallmatrix}\right]}(\tau_K)^2 / g_{\left[\begin{smallmatrix}1/2\\0\end{smallmatrix}\right]}(\tau_K)^2$$

belongs to $K_{4\mathcal{O}_K}$ by lemma 2.3 and proposition 5.1, the value

$$\zeta_{2N} g_{\left[\begin{smallmatrix}1/2\\1/2+1/N\end{smallmatrix}\right]}(\tau_K)^2 / g_{\left[\begin{smallmatrix}0\\1/N\end{smallmatrix}\right]}(\tau_K)^2$$

generates $K_{\mathfrak{n}}$ over $K_{4\mathcal{O}_K}$.

Example 6.4. Let $K = \mathbb{Q}(\sqrt{-10})$ and let $\mathfrak{n} = 4\mathcal{O}_K$. Consider the special value

$$x = \zeta_8^7 g_{\left[\begin{smallmatrix}1/2\\3/4\end{smallmatrix}\right]}(\sqrt{-10})^2 / g_{\left[\begin{smallmatrix}0\\1/4\end{smallmatrix}\right]}(\sqrt{-10})^2.$$

This value generates $K_{\mathfrak{n}}$ over H_K as an algebraic unit by theorem 6.2. Furthermore, since x is a real number by (2.3), we see that

$$[K(x):K] = [K(x):\mathbb{Q}]/[K:\mathbb{Q}] = [K(x):\mathbb{Q}(x)][\mathbb{Q}(x):\mathbb{Q}]/[K:\mathbb{Q}] = [\mathbb{Q}(x):\mathbb{Q}].$$

Hence, the minimal polynomial of x over K has integer coefficients. By using proposition 5.2, [11] and [4, ch. 2, § 1] one can readily find all the Galois conjugates of x

over K (possibly with some multiplicity) as follows:

$$\begin{aligned}
x_1 &= \zeta_8^7 g_{\left[\begin{smallmatrix}1/2\\3/4\end{smallmatrix}\right]}(\sqrt{-10})^2/g_{\left[\begin{smallmatrix}0\\1/4\end{smallmatrix}\right]}(\sqrt{-10})^2,\\
x_2 &= \zeta_8^5 g_{\left[\begin{smallmatrix}1/4\\3/4\end{smallmatrix}\right]}(\sqrt{-10})^2/g_{\left[\begin{smallmatrix}1/4\\1/4\end{smallmatrix}\right]}(\sqrt{-10})^2,\\
x_3 &= \zeta_8^3 g_{\left[\begin{smallmatrix}0\\3/4\end{smallmatrix}\right]}(\sqrt{-10})^2/g_{\left[\begin{smallmatrix}1/2\\1/4\end{smallmatrix}\right]}(\sqrt{-10})^2,\\
x_4 &= \zeta_8^7 g_{\left[\begin{smallmatrix}3/4\\3/4\end{smallmatrix}\right]}(\sqrt{-10})^2/g_{\left[\begin{smallmatrix}3/4\\1/4\end{smallmatrix}\right]}(\sqrt{-10})^2,\\
x_5 &= \zeta_8 g_{\left[\begin{smallmatrix}3/4\\1/2\end{smallmatrix}\right]}(\sqrt{-10}/2)^2/g_{\left[\begin{smallmatrix}1/4\\0\end{smallmatrix}\right]}(\sqrt{-10}/2)^2,\\
x_6 &= \zeta_8 g_{\left[\begin{smallmatrix}3/4\\3/4\end{smallmatrix}\right]}(\sqrt{-10}/2)^2/g_{\left[\begin{smallmatrix}1/4\\3/4\end{smallmatrix}\right]}(\sqrt{-10}/2)^2,\\
x_7 &= \zeta_8^5 g_{\left[\begin{smallmatrix}3/4\\0\end{smallmatrix}\right]}(\sqrt{-10}/2)^2/g_{\left[\begin{smallmatrix}1/4\\1/2\end{smallmatrix}\right]}(\sqrt{-10}/2)^2,\\
x_8 &= \zeta_8^3 g_{\left[\begin{smallmatrix}3/4\\1/4\end{smallmatrix}\right]}(\sqrt{-10}/2)^2/g_{\left[\begin{smallmatrix}1/4\\1/4\end{smallmatrix}\right]}(\sqrt{-10}/2)^2.
\end{aligned}$$

One can also compute (by using Maple v. 16) $\min(x, K)$ as

$$\prod_{k=1}^{8}(X - x_k) = X^8 - 72X^7 + 12X^6 + 72X^5 + 38X^4 + 72X^3 + 12X^2 - 72X + 1,$$

which is irreducible over $\mathbb{Q}$. Therefore, x generates $K_{\mathfrak{n}}$ even over K as a unit. Here, we observe that the coefficients of $\min(x, K)$ are much smaller than those of

$$\begin{aligned}
&\min\left(g_{\left[\begin{smallmatrix}0\\1/4\end{smallmatrix}\right]}(\sqrt{-10})^{12\cdot 4}, K\right)\\
&\quad = X^8 - 18119554025681772 8X^7 - 577566311456260690 6112X^6\\
&\qquad - 2703546469163737745736089 6X^5 + 54133907603074109682154565632 0X^4\\
&\qquad - 12493761534308794479534255610265 6X^3\\
&\qquad + 156619184734352277132318185598484 48X^2\\
&\qquad - 328318164045274003236441485402439 68X + 16777216.
\end{aligned}$$

Acknowledgements

H.Y.J. was supported by the National Institute for Mathematical Sciences (NIMS) grant funded by the Korean government (Grant no. C21601). D.H.S. was supported by the Hankuk University of Foreign Studies Research Fund of 2014.

References

1 S. Bettner and R. Schertz. Lower powers of elliptic units. *J. Théorie Nombres Bordeaux* **13** (2001), 339–351.

2 B. Cho. Siegel–Ramachandra invariants generate ray class fields. *J. Math. Analysis Applic.* **401** (2013), 293–297.

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

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

5 S. Lang. *Elliptic functions*, 2nd edn. Graduate Texts in Mathematics, vol. 112 (Springer, 1987).

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

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

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

9 G. Shimura. *Introduction to the arithmetic theory of automorphic functions* (Iwanami Shoten/Princeton University Press, 1971).

10 J. H. Silverman. *The arithmetic of elliptic curves*. Graduate Texts in Mathematics, vol. 106 (Springer, 1992).

11 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).