Construction of class fields over cyclotomic fields

Ja Kyung Koo and Dong Sung Yoon

Abstract Let ℓ and p be odd primes. For a positive integer μ, let k_μ be the ray class field of $k = \mathbb{Q}(e^{2\pi i/\ell})$ modulo $2p^\mu$. We present certain class fields K_μ of k such that $k_\mu \subset K_\mu \subset k_{\mu+1}$, and we provide a necessary and sufficient condition for $K_\mu = k_{\mu+1}$. We also construct, in the sense of Hilbert, primitive generators of the field K_μ over k_μ by using Shimura's reciprocity law and special values of theta constants.

1. Introduction

In his 12th problem, Hilbert asked what kind of analytic functions and algebraic numbers are necessary to construct all abelian extensions of given number fields. For any number field K and a modulus $\mathfrak{m}$ of K, it is well known (see [29] or [7, Theorem 8.6]) that there is a unique maximal abelian extension of K unramified outside $\mathfrak{m}$, which is called the *ray class field* of K modulo $\mathfrak{m}$. Hence, as a first step toward the problem we need to construct ray class fields for given number fields. Historically, over imaginary quadratic number fields K, Hasse [10] constructed the ray class field of K by making use of the Weber function and the elliptic modular function. After Hasse, many people investigated this theme (see, e.g., [2]–[9], [12], [18], [20]–[22], [28]). On the other hand, over any other CM-fields K with $[K:\mathbb{Q}] > 2$, not much seems to be known so far. For instance, over a cyclotomic number field K with odd relative class number, Shimura [23] showed that the Hilbert class field of K is generated by that of the maximal real subfield of K and the unramified abelian extensions of K obtained by the fields of moduli of two certain polarized abelian varieties having subfields of K as endomorphism algebras. By making use of Galois representation, Ribet [19] constructed unramified abelian, degree-p extensions of $K = \mathbb{Q}(e^{2\pi i/p})$ for all irregular primes p (see also [17]). Furthermore, Komatsu [14] investigated a certain class field of $K = \mathbb{Q}(e^{2\pi i/5})$ and constructed its normal basis by means of Siegel modular functions.

Now, let n be a positive integer, let k be a CM-field with $[k:\mathbb{Q}] = 2n$, let k^* be its reflex field, and let z_0 be the associated CM-point (see Section 3). Shimura [27] showed that if f is a Siegel modular function which is finite at z_0, then the

Kyoto Journal of Mathematics, Vol. 56, No. 4 (2016), 803–829
DOI 10.1215/21562261-3664923, © 2016 by Kyoto University
Received August 31, 2015. Revised October 26, 2015. Accepted November 4, 2015.
2010 Mathematics Subject Classification: Primary 11R37, 11F46; Secondary 11G15, 14H42.

special value $f(z_0)$ belongs to some abelian extension (i.e., class field) of k^*. His reciprocity law explains Galois actions on $f(z_0)$ in terms of the action of the group $G_{\mathbb{A}+}$ on f (Proposition 3.2). Here $G_{\mathbb{A}+} = \prod'_p \mathrm{GSp}_{2n}(\mathbb{Q}_p) \times \mathrm{GSp}^+_{2n}(\mathbb{R})$ is the restricted product with respect to the subgroups $\mathrm{GSp}_{2n}(\mathbb{Z}_p)$ of $\mathrm{GSp}_{2n}(\mathbb{Q}_p)$. Shimura [26] also constructed Siegel modular functions by the quotient of two theta constants

$$\Phi_{(r,s)}(z) = \frac{\sum_{x\in\mathbb{Z}^n} e(\frac{1}{2}{}^t(x+r)z(x+r) + {}^t(x+r)s)}{\sum_{x\in\mathbb{Z}^n} e(\frac{1}{2}{}^t xzx)},$$

for $r, s \in \mathbb{Q}^n$, and explicitly described the Galois actions on the special values of theta functions (see Section 5).

In this article, we mainly consider the case of cyclotomic number fields $k = \mathbb{Q}(e^{2\pi i/\ell})$ for any odd prime ℓ. Let p be an odd prime, and let μ be a positive integer. We denote by k_μ the ray class field of k modulo $2p^\mu$. In Section 4, we define the class field K_μ of k such that $k_\mu \subset K_\mu \subset k_{\mu+1}$, which would be an extension of Komatsu's result [14, Proposition 1]. We shall first find the exact degree of K_μ over k_μ for any odd prime ℓ (Theorem 4.5). We shall further provide a necessary and sufficient condition for K_μ to be the ray class field $k_{\mu+1}$ (Corollary 4.6). In Section 6, as Hilbert proposed, by using Shimura's reciprocity law we shall construct a primitive generator of K_μ/k_μ in terms of a special value of $\Phi_{(r,s)}(z)$ for some $r, s \in \mathbb{Q}^n$ at the CM-point corresponding to the polarized abelian variety of genus $n = (\ell-1)/2$ (Theorem 6.4).

NOTATION 1.1

For $z \in \mathbb{C}$, we denote by $\overline{z}$ the complex conjugate of z and by $\mathrm{Im}(z)$ the imaginary part of z, and we put $e(z) = e^{2\pi i z}$. If R is a ring with identity and $r, s \in \mathbb{Z}_{>0}$, then $M_{r\times s}(R)$ indicates the ring of all $r \times s$ matrices with entries in R. In particular, we set $M_r(R) = M_{r\times r}(R)$. The identity matrix of $M_r(R)$ is written as 1_r, and the transpose of a matrix α is denoted by ${}^t\alpha$. Additionally, $R^\times$ stands for the group of all invertible elements of R. When G is a group and $g_1, g_2, \ldots, g_r$ are elements of G, let $\langle g_1, g_2, \ldots, g_r\rangle$ be the subgroup of G generated by $g_1, g_2, \ldots, g_r$, and let G^n be the subgroup $\{g^n \mid g \in G\}$ of G for $n \in \mathbb{Z}_{>0}$. Moreover, when H is a subgroup of G, let $|G : H|$ be the index of H in G. For a finite algebraic extension K over F, $[K : F]$ denotes the degree of K over F. We let $\zeta_N = e^{2\pi i/N}$ be a primitive Nth root of unity for a positive integer N.

2. Siegel modular forms

We shall briefly present necessary facts about Siegel modular forms and explain the action of $G_{\mathbb{A}+}$ on the Siegel modular functions whose Fourier coefficients lie in some cyclotomic fields.

Let n be a positive integer, and let G be the algebraic subgroup of GL_{2n} defined over $\mathbb{Q}$ such that

$$G_{\mathbb{Q}} = \left\{\alpha \in \mathrm{GL}_{2n}(\mathbb{Q}) \,\middle|\, {}^t\alpha J\alpha = \nu(\alpha)J \text{ with } \nu(\alpha) \in \mathbb{Q}^\times\right\},$$

where

$$J = J_n = \begin{bmatrix} 0 & -1_n \\ 1_n & 0 \end{bmatrix}.$$

Let $G_{\mathbb{A}}$ be the adelization of G, let G_0 be the non-Archimedean part of $G_{\mathbb{A}}$, and let G_∞ be the archimedean part of $G_{\mathbb{A}}$. We extend the multiplier map $\nu : G_{\mathbb{Q}} \to \mathbb{Q}^\times$ to a continuous map of $G_{\mathbb{A}}$ into $\mathbb{Q}_{\mathbb{A}}^\times$, which we denote again by ν. Then we put $G_{\infty+} = \{x \in G_\infty \mid \nu(x) \gg 0\}$ and $G_{\mathbb{A}+} = G_0 G_{\infty+}$. Here $t \gg 0$ means $t_v > 0$ for all archimedean primes v of $\mathbb{Q}$. For a positive integer N, let

$$R_N = \mathbb{Q}^\times \cdot \Big\{ a \in G_{\mathbb{A}+} \,\Big|\, a_q \in \mathrm{GL}_{2n}(\mathbb{Z}_q), a_q \equiv 1_{2n} \pmod{N \cdot M_{2n}(\mathbb{Z}_q)} \text{ for all primes } q \Big\},$$

$$\Delta = \left\{ \begin{bmatrix} 1_n & 0 \\ 0 & x \cdot 1_n \end{bmatrix} \,\middle|\, x \in \prod_q \mathbb{Z}_q^\times \right\},$$

$$G_{\mathbb{Q}+} = \big\{ \alpha \in G_{\mathbb{Q}} \,\big|\, \nu(\alpha) > 0 \big\}.$$

PROPOSITION 2.1

For every positive integer N, we have

$$G_{\mathbb{A}+} = R_N \Delta G_{\mathbb{Q}+}.$$

Proof

See [24, Proposition 3.4] and [25, p. 535, (3.10.3)]. □

Let $\mathbb{H}_n = \{z \in M_n(\mathbb{C}) \mid {}^t z = z, \mathrm{Im}(z) > 0\}$ be the Siegel upper half-space of degree n. Here, for a Hermitian matrix ξ we write $\xi > 0$ to mean that ξ is positive definite. We define the action of an element $\alpha = \left[\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right]$ of $G_{\mathbb{Q}+}$ on $\mathbb{H}_n$ by

$$\alpha(z) = (Az + B)(Cz + D)^{-1},$$

where $A, B, C, D \in M_n(\mathbb{Q})$. For every positive integer N, let

$$\Gamma(N) = \big\{ \gamma \in \mathrm{Sp}_{2n}(\mathbb{Z}) \,\big|\, \gamma \equiv 1_{2n} \pmod{N \cdot M_{2n}(\mathbb{Z})} \big\}.$$

For an integer m, a holomorphic function $f : \mathbb{H}_n \to \mathbb{C}$ is called a (classical) *Siegel modular form of weight m and level N* if

$$f\big(\gamma(z)\big) = \det(Cz + D)^m f(z) \tag{2.1}$$

for all $\gamma = \left[\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right] \in \Gamma(N)$ and $z \in \mathbb{H}_n$, plus the requirement when $n = 1$ that f is holomorphic at every cusp. In particular, $f(z)$ has a Fourier expansion of the form

$$f(z) = \sum_\xi A(\xi) e\big(\mathrm{tr}(\xi z)/N\big)$$

with $A(\xi) \in \mathbb{C}$, where ξ runs over all positive semidefinite half-integral symmetric matrices of degree n (see [13, Section 4, Theorem 1]). Here, a symmetric matrix

$\xi \in M_n(\mathbb{Q})$ is called *half-integral* if 2ξ is an integral matrix whose diagonal entries are even.

For a subring R of $\mathbb{C}$, let $\mathcal{M}_m(\Gamma(N), R)$ be the vector space of all Siegel modular forms f of weight m and level N whose Fourier coefficients $A(\xi)$ belong to R, and let $\mathcal{M}_m(R) = \bigcup_{N=1}^{\infty} \mathcal{M}_m(\Gamma(N), R)$. We denote by $\mathcal{A}_m(R)$ the set of all meromorphic functions of the form g/h with $g \in \mathcal{M}_{r+m}(R)$, $0 \neq h \in \mathcal{M}_r(R)$ (with any $r \in \mathbb{Z}$), and we denote by $\mathcal{A}_m(\Gamma(N), R)$ the set of all $f \in \mathcal{A}_m(R)$ satisfying (2.1). In particular, we set

$$\mathcal{F}_N = \mathcal{A}_0\big(\Gamma(N), \mathbb{Q}(\zeta_N)\big),$$

$$\mathcal{F} = \bigcup_{N=1}^{\infty} \mathcal{F}_N.$$

For every algebraic number field K, let K_{ab} be the maximal abelian extension of K, and let $K_{\mathbb{A}}^{\times}$ be the idèle group of K. By class field theory, every element x of $K_{\mathbb{A}}^{\times}$ acts on K_{ab} as an automorphism. We then denote this automorphism by $[x, K]$. On the other hand, every element of $G_{\mathbb{A}+}$ acts on $\mathcal{F}$ as an automorphism (see [26, p. 680]). If $x \in G_{\mathbb{A}+}$ and $f \in \mathcal{F}$, then we denote by f^x the image of f under x.

PROPOSITION 2.2

Let $f(z) = \sum_{\xi} A(\xi) e(\mathrm{tr}(\xi z)/N) \in \mathcal{F}_N$. Then we get the following.

(i) *$f^{\beta} = f$ for $\beta \in R_N$. Moreover, $\mathcal{F}_N$ is the subfield of $\mathcal{F}$ consisting of all the R_N-invariant elements.*

(ii) *Let $y = \left[\begin{smallmatrix} 1_n & 0 \\ 0 & x \cdot 1_n \end{smallmatrix}\right] \in \Delta$, and let t be a positive integer such that $t \equiv x_q \pmod{N\mathbb{Z}_q}$ for all primes q. Then we derive*

$$f^y = \sum_{\xi} A(\xi)^{\sigma} e\big(\mathrm{tr}(\xi z)/N\big),$$

where σ is the automorphism of $\mathbb{Q}(\zeta_N)$ such that $\zeta_N^{\sigma} = \zeta_N^t$.

(iii) *$f^{\alpha} = f \circ \alpha$ for $\alpha \in G_{\mathbb{Q}+}$.*

Proof

See [26, p. 681] and [27, Theorem 26.8]. □

3. Shimura's reciprocity law

We begin with fundamental but necessary facts about Shimura's reciprocity law from [27, Section 26]. Let n be a positive integer, let K be a CM-field with $[K : \mathbb{Q}] = 2n$, and let $\mathcal{O}_K$ be a ring of integers of K. Let $\varphi_1, \varphi_2, \ldots, \varphi_n$ be n distinct embeddings of K into $\mathbb{C}$ such that there are no two embeddings among them which are complex conjugates of each other on K. Then $(K; \{\varphi_1, \varphi_2, \ldots, \varphi_n\})$ is a CM-type, and we can take an element ρ in K such that

(i) ρ is purely imaginary,

(ii) $\mathrm{Im}(\rho^{\varphi_i}) > 0$ for all $i = 1, \dots, n$,
(iii) $\mathrm{Tr}_{K/\mathbb{Q}}(\rho\xi) \in \mathbb{Z}$ for all $\xi \in \mathcal{O}_K$.

We denote by $v(x)$, for $x \in K$, the vector of $\mathbb{C}^n$ whose components are $x^{\varphi_1}, \dots, x^{\varphi_n}$. The set $L = \{v(x) \mid x \in \mathcal{O}_K\}$ is a lattice in $\mathbb{C}^n$. We define an $\mathbb{R}$-bilinear form $E(z, w)$ on $\mathbb{C}^n$ by

$$E(z,w) = \sum_{i=1}^{n} \rho^{\varphi_i}(z_i\overline{w_i} - \overline{z_i}w_i) \quad \text{for } z = \begin{bmatrix} z_1 \\ \vdots \\ z_n \end{bmatrix} \text{ and } w = \begin{bmatrix} w_1 \\ \vdots \\ w_n \end{bmatrix}.$$

Then E becomes a nondegenerate Riemann form on the complex torus $\mathbb{C}^n/L$ satisfying

$$E\big(v(x), v(y)\big) = \mathrm{Tr}_{k/\mathbb{Q}}(\rho x\overline{y}) \quad \text{for } x, y \in K,$$

which makes it a polarized abelian variety (see [27, pp. 43–44]). Hence, we can find a positive integer δ, a diagonal matrix ϵ with integral elements, and a complex $n \times 2n$ matrix Ω such that (see [27, Lemma 27.2] or [26, p. 675])

(i) $E(\Omega x, \Omega y) = \delta \cdot {}^t x J y$ for $x, y \in \mathbb{R}^{2n}$,
(ii) $L = \{\Omega \left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right] \mid a \in \mathbb{Z}^n, b \in \epsilon\mathbb{Z}^n\}$,
(iii)

$$\epsilon = \begin{bmatrix} \epsilon_1 & & & \\ & \epsilon_2 & & \\ & & \ddots & \\ & & & \epsilon_n \end{bmatrix}, \quad \epsilon_1 = 1, \epsilon_i \mid \epsilon_{i+1}, \text{for } i = 1, \dots, n-1.$$

Now, we write $\Omega = [\Omega_1\ \Omega_2] = [v(e_1)\ v(e_2)\ \cdots\ v(e_{2n})]$ with $\Omega_1, \Omega_2 \in M_n(\mathbb{C})$ and $e_1, e_2, \dots, e_{2n} \in K$, and we put $z_0 = \Omega_2^{-1}\Omega_1$. It is well known that $z_0 \in \mathbb{H}_n$. Let $\Phi : K \to M_n(\mathbb{C})$ be a ring monomorphism such that

$$\Phi(x) = \begin{bmatrix} x^{\varphi_1} & & & \\ & x^{\varphi_2} & & \\ & & \ddots & \\ & & & x^{\varphi_n} \end{bmatrix} \quad \text{for } x \in K.$$

Then we can define a ring monomorphism $h : K \to M_{2n}(\mathbb{Q})$ by

$$\Phi(x)\Omega = \Omega \cdot {}^t h(x) \quad \text{for } x \in K.$$

Here, $h(x) = [a_{ij}]_{1 \le i,j \le 2n}$ is, in fact, the regular representation of x with respect to $\{e_1, e_2, \dots, e_{2n}\}$, namely, $xe_i = \sum_{j=1}^{2n} a_{ij}e_j$. If $\epsilon = 1_n$, then $L = v(\mathcal{O}_K) = \Omega \cdot \mathbb{Z}^{2n} = \mathbb{Z}v(e_1) + \cdots + \mathbb{Z}v(e_{2n})$ so that $h(x) \in M_{2n}(\mathbb{Z})$ for $x \in \mathcal{O}_K$. One can then readily show that

$$h(\overline{x}) = J^t h(x) J^{-1} \quad \text{for } x \in K,$$

and that z_0 is the CM-point of $\mathbb{H}_n$ induced from h which corresponds to the principally polarized abelian variety $(\mathbb{C}^n/L, E)$ (see [26, pp. 684–685] or [27,

Section 24.10]). In particular, if we set $S = \{x \in K^\times \mid x\overline{x} \in \mathbb{Q}^\times\}$, then $h(S) = \{h(s) \mid s \in S\} = \{\alpha \in G_{\mathbb{Q}+} \mid \alpha(z_0) = z_0\}$.

Let K^* be the reflex field of K, let K' be a Galois extension of K over $\mathbb{Q}$, and extend φ_i $(i = 1, \dots, n)$ to an element of $\mathrm{Gal}(K'/\mathbb{Q})$, which we denote again by φ_i. Let $\{\psi_j\}_{j=1}^m$ be the set of all embeddings of K^* into $\mathbb{C}$ obtained from $\{\varphi_i^{-1}\}_{i=1}^n$.

PROPOSITION 3.1

Let K, K^*, and $\{\psi_j\}$ be as above.

(i) *$(K^*; \{\psi_1, \dots, \psi_m\})$ is a primitive CM-type and we have*

$$K^* = \mathbb{Q}\Big(\sum_{i=1}^n x^{\varphi_i} \,\Big|\, x \in K\Big).$$

(ii) *If $b = \prod_j a^{\psi_j}$ with $a \in K^*$, then $b \in K$ and $b\overline{b} = N_{K^*/\mathbb{Q}}(a)$.*

Proof

See [27, pp. 62–63]. □

We call the CM-type $(K^*; \{\psi_j\})$ the *reflex* of $(K; \{\varphi_i\})$. By Proposition 3.1, we can define a homomorphism $\varphi^* : (K^*)^\times \to K^\times$ by

$$\varphi^*(a) = \prod_{j=1}^m a^{\psi_j} \quad \text{for } a \in (K^*)^\times,$$

and we have $\varphi^*(a) \cdot \overline{\varphi^*(a)} = N_{K^*/\mathbb{Q}}(a)$ for $a \in (K^*)^\times$. The map h can be extended naturally to a homomorphism $K_{\mathbb{A}} \to M_{2n}(\mathbb{Q}_{\mathbb{A}})$, which we also denote by h. Then for every $b \in (K^*)_{\mathbb{A}}^\times$ we get $\nu(h(\varphi^*(b))) = N_{K^*/\mathbb{Q}}(b)$ and $h(\varphi^*(b)^{-1}) \in G_{\mathbb{A}+}$ (see [27, p. 172]).

PROPOSITION 3.2 (SHIMURA'S RECIPROCITY LAW)

Let K, h, z_0, and K^* be as above. Then for every $f \in \mathcal{F}$ which is finite at z_0, the value $f(z_0)$ belongs to K_{ab}^*. Moreover, if $b \in (K^*)_{\mathbb{A}}^\times$, then $f^{h(\varphi^*(b)^{-1})}$ is finite at z_0 and

$$f(z_0)^{[b,K^*]} = f^{h(\varphi^*(b)^{-1})}(z_0).$$

Proof

See [27, Theorem 26.8]. □

REMARK 3.3

For any $f \in \mathcal{F}$ which is finite at z_0, the value $f(z_0)$ in fact belongs to the class field $\widetilde{K_{ab}^*}$ of K^* corresponding to the kernel of φ^*.

4. Class fields over cyclotomic fields

Let ℓ and p be odd prime numbers. We also write for simplicity $\zeta = \zeta_\ell$. Set $k = \mathbb{Q}(\zeta)$ and $n = (\ell-1)/2$ so that $2n = [k : \mathbb{Q}]$. For $1 \le i \le 2n$ we denote by φ_i the element of $\mathrm{Gal}(k/\mathbb{Q})$ defined by $\zeta^{\varphi_i} = \zeta^i$. Then $(k; \{\varphi_1, \varphi_2, \dots, \varphi_n\})$ is a primitive CM-type and $(k; \{\varphi_1^{-1}, \varphi_2^{-1}, \dots, \varphi_n^{-1}\})$ is its reflex (see [27, p. 64]). For a positive integer μ, put

$$S_\mu = \left\{ a \in k^\times \;\middle|\; a \equiv 1 \pmod{2p^\mu} \right\},$$
$$\widetilde{S_\mu} = \left\{ (a) \;\middle|\; a \in S_\mu \right\},$$

where (a) is the principal ideal of k generated by a. Let E be the unit group of k, and let k_μ be the ray class field of k modulo $2p^\mu$. Then we have

$$\mathrm{Gal}(k_{\mu+1}/k_\mu) \cong \widetilde{S_\mu}/\widetilde{S_{\mu+1}} \cong S_\mu E/S_{\mu+1}E \cong S_\mu/S_{\mu+1}(S_\mu \cap E)$$

by class field theory. Further, we set $H_\mu = S_{\mu+1}(S_\mu \cap E)$ and

$$\omega_{\mu,i} = \begin{cases} 1 + 2p^\mu \zeta^i & \text{for } 1 \le i \le n+1, \\ 1 + 2p^\mu(\zeta^n + \zeta^{n+1} - \zeta^i - \zeta^{-i}) & \text{for } n+2 \le i \le 2n. \end{cases}$$

Since the ring of integers $\mathcal{O}_k$ of k is equal to $\mathbb{Z}[\zeta]$ and $S_\mu/S_{\mu+1}$ is isomorphic to $\mathcal{O}_k/p\mathcal{O}_k$ by a mapping

$$S_\mu/S_{\mu+1} \longrightarrow \mathcal{O}_k/p\mathcal{O}_k,$$
$$(1 + 2p^\mu\omega)S_{\mu+1} \longmapsto \omega + p\mathcal{O}_k \quad \text{for } \omega \in \mathcal{O}_k,$$

we obtain $S_\mu/S_{\mu+1} \cong (\mathbb{Z}/p\mathbb{Z})^{2n}$ and

$$S_\mu/S_{\mu+1} = \left\langle (1+2p^\mu\zeta)S_\mu, (1+2p^\mu\zeta^2)S_\mu, \dots, (1+2p^\mu\zeta^{2n})S_\mu \right\rangle.$$

Let $B = [b_{ij}] \in M_{2n}(\mathbb{Z})$ where b_{ij} is an integer such that $\omega_{\mu,i} = 1 + 2p^\mu(\sum_{j=1}^{2n} b_{ij}\zeta^j)$. Then we get

$$B = \left[\begin{array}{ccccc|cccc} 1 & & & & & 0 & 0 & \cdots & 0 \\ & 1 & & & & \vdots & \vdots & & \vdots \\ & & \ddots & & & \vdots & \vdots & & \vdots \\ & & & & 1 & 0 & 0 & \cdots & 0 \\ \hline & & & 0 & & 1 & & & \\ & & -1 & 1 & & 1 & -1 & & \\ & \iddots & & \vdots & & \vdots & & \ddots & \\ -1 & & & 1 & & 1 & & & -1 \end{array}\right].$$

Hence, $S_\mu/S_{\mu+1} = \langle \omega_{\mu,1}S_{\mu+1}, \omega_{\mu,2}S_{\mu+1}, \dots, \omega_{\mu,2n}S_{\mu+1} \rangle$ because $\det(B) = (-1)^{n-1}$ is prime to p. This shows that $S_\mu/H_\mu = \langle \omega_{\mu,1}H_\mu, \omega_{\mu,2}H_\mu, \dots, \omega_{\mu,2n}H_\mu \rangle$ due to the fact that $H_\mu \supset S_{\mu+1}$.

Now, we define an endomorphism φ^* of $k^\times$ by

$$\varphi^*(a) = \prod_{i=1}^{n} a^{\varphi_i^{-1}} \quad \text{for } a \in k^\times$$

and an endomorphism φ^+ of k by

$$\varphi^+(a) = \sum_{i=1}^{n} a^{\varphi_i^{-1}} \quad \text{for } a \in k.$$

We let

$$\eta_{\mu,i} = \begin{cases} 1 + 2p^{\mu}\varphi^+(\zeta^i) & \text{for } 1 \le i \le n+1, \\ 1 & \text{for } n+2 \le i \le 2n, \end{cases}$$

so that $\varphi^*(\omega_{\mu,i})H_\mu = \eta_{\mu,i}H_\mu$ for all $1 \le i \le 2n$. Since $\varphi^*(H_\mu) \subset H_\mu$, we can define an endomorphism $\widetilde{\varphi_\mu^*}$ of S_μ/H_μ by $\widetilde{\varphi_\mu^*}(aH_\mu) = \varphi^*(a)H_\mu$. Let K_μ be the class field of k corresponding to the kernel of $\widetilde{\varphi_\mu^*}$. Note that $K_\mu = k_\mu(k_{\mu+1} \cap \widetilde{k_{ab}})$, where $\widetilde{k_{ab}}$ is the class field of k in Remark 3.3. Then we get

$$\begin{aligned} \mathrm{Gal}(K_\mu/k_\mu) &\cong (S_\mu/H_\mu)/\ker(\widetilde{\varphi_\mu^*}) \cong \widetilde{\varphi_\mu^*}(S_\mu/H_\mu) \\ &= \langle \eta_{\mu,1}H_\mu, \eta_{\mu,2}H_\mu, \ldots, \eta_{\mu,n+1}H_\mu \rangle. \end{aligned} \tag{4.1}$$

Observe that K_μ is the fixed field of $\{(\frac{k_{\mu+1}/k}{(\omega)}) \mid \omega H_\mu \in \ker(\widetilde{\varphi_\mu^*})\}$ and

$$\mathrm{Gal}(K_\mu/k_\mu) = \left\langle \left(\frac{K_\mu/k}{(\omega_{\mu,1})}\right), \left(\frac{K_\mu/k}{(\omega_{\mu,2})}\right), \ldots, \left(\frac{K_\mu/k}{(\omega_{\mu,n+1})}\right) \right\rangle.$$

Here, $(\frac{k_{\mu+1}/k}{\cdot})$ is the Artin map of $k_{\mu+1}/k$.

PROPOSITION 4.1

Let N be a positive integer, let $K = \mathbb{Q}(\zeta_N)$, and let K^+ be its maximal real subfield. Let E (resp., E^+) be the unit group of K (resp., K^+), and let W be the group of roots of unity in K. Then we have

$$|E : WE^+| = \begin{cases} 1 & \text{if } N \text{ is a prime power}, \\ 2 & \text{if } N \text{ is not a prime power}. \end{cases}$$

Proof

See [30, Corollary 4.13]. □

PROPOSITION 4.2

Let ℓ be any prime, and let $m \in \mathbb{Z}_{>0}$. Let $\mathbb{Q}(\zeta_{\ell^m})^+$ be the maximal real subfield of $\mathbb{Q}(\zeta_{\ell^m})$, and let $E_{\ell^m}^+$ be its unit group. Further, we let $C_{\ell^m}^+$ be the subgroup of $E_{\ell^m}^+$ generated by -1 and the real units

$$\xi_a = \zeta_{2\ell^m}^{1-a} \cdot \frac{1-\zeta_{\ell^m}^a}{1-\zeta_{\ell^m}} \in \mathbb{R}, \quad 1 < a < \frac{\ell^m}{2}, \quad \gcd(a,\ell) = 1.$$

Then

$$h_{\ell^m}^+ = |E_{\ell^m}^+ : C_{\ell^m}^+|,$$

where $h_{\ell^m}^+$ is the class number of $\mathbb{Q}(\zeta_{\ell^m})^+$.

Proof
See [30, Lemma 8.1 and Theorem 8.2]. □

LEMMA 4.3
Let ℓ be an odd prime, and let p be an odd prime such that $p \nmid \ell h_\ell^+$, where h_ℓ^+ is the class number of the maximal real subfield of k. Then $H_\mu/S_{\mu+1}$ is generated by real units of k for all $\mu \in \mathbb{Z}_{>0}$.

Proof
The $(2\ell h_\ell^+)$th power mapping of $S_\mu/S_{\mu+1}$ induces an automorphism of itself because $\gcd(p, 2\ell h_\ell^+) = 1$. Thus, the image of $E \cap S_\mu$ in $S_\mu/S_{\mu+1}$ is the same as that of $E^{2\ell h_\ell^+} \cap S_\mu$. By Propositions 4.1 and 4.2, $E^{2\ell h_\ell^+} \subset \langle \xi_a^{2\ell} \mid 1 < a < \ell/2 \rangle$ where $\xi_a = \zeta_{2\ell}^{1-a}(1-\zeta^a)/(1-\zeta) \in \mathbb{R}$. Therefore, $H_\mu/S_{\mu+1} = S_{\mu+1}(E^{2\ell h_\ell^+} \cap S_\mu)/S_{\mu+1}$ is generated by real units of k. □

Let $M_\ell(p) = [m_{ij}] \in M_{(n+1)\times 2n}(\mathbb{Z}/p\mathbb{Z})$, where m_{ij} is the coefficient of ζ^j in $\varphi^+(\zeta^i)$ in $\mathbb{Z}/p\mathbb{Z}$. Then we get

$$m_{ij} = \begin{cases} 1 & \text{if } \overline{i} \cdot \overline{j}^{-1} \in \{\overline{1}, \overline{2}, \dots, \overline{n}\} \text{ in } \mathbb{Z}/\ell\mathbb{Z}, \\ 0 & \text{otherwise.} \end{cases}$$

We can then easily see that the rank of $M_\ell(p)$ is equal to the dimension of the vector subspace $\langle \eta_{\mu,1} S_{\mu+1}, \eta_{\mu,2} S_{\mu+1}, \dots, \eta_{\mu,n+1} S_{\mu+1} \rangle$ in $S_\mu/S_{\mu+1}$.

LEMMA 4.4
Let ℓ and p be odd primes, and let $\mu \in \mathbb{Z}_{>0}$. For $1 \le i, j \le 2n$, let

$$n_{ij} = \begin{cases} 1 & \text{if } \overline{i} \cdot \overline{j} \in \{\overline{1}, \overline{2}, \dots, \overline{n}\} \text{ in } \mathbb{Z}/\ell\mathbb{Z}, \\ 0 & \text{otherwise,} \end{cases}$$

and let $N_\ell = [n_{ij}]_{1 \le i,j \le n} \in M_n(\mathbb{Z})$. Then the images $\eta_{\mu,1}, \eta_{\mu,2}, \dots, \eta_{\mu,n+1}$ are linearly independent in $S_\mu/S_{\mu+1}$ if and only if $p \nmid \det(N_\ell)$.

Proof
Let $N'_\ell = [n_{ij}]_{1 \le i \le n+1, 1 \le j \le 2n} \in M_{(n+1)\times 2n}(\mathbb{Z}/p\mathbb{Z})$. It is clear that $\operatorname{rank}(M_\ell(p)) = \operatorname{rank}(N'_\ell)$. Hence, the images $\eta_{\mu,1}, \eta_{\mu,2}, \dots, \eta_{\mu,n+1}$ are linearly independent in $S_\mu/S_{\mu+1}$ if and only if N'_ℓ has rank $n+1$. Now, we claim that $\operatorname{rank}(N'_\ell) = n+1$ if and only if N'_ℓ induces the following row echelon form:

$$\begin{bmatrix} 1 & & & & & & & -1 \\ & 1 & & & & & -1 & \\ & & \ddots & & & \iddots & & \\ & & & 1 & -1 & & & \\ & & & & 1 & 1 & \cdots & 1 \end{bmatrix}. \tag{4.2}$$

The "if" part is obvious. Note that if $n_{ij} = 1$ (resp., 0), then $n_{i\ell-j} = 0$ (resp., 1) because there are no two automorphisms among $\varphi_1, \varphi_2, \dots, \varphi_n$ which are complex

conjugates of each other. Let v_i be the ith row vector of N'_ℓ for $1 \le i \le n+1$, and let

$$v'_i = [v'_{ij}]_{1\le j\le 2n} = \begin{cases} 2v_i - v_n - v_{n+1} & \text{for } 1 \le i \le n, \\ v_n + v_{n+1} & \text{for } i = n+1. \end{cases}$$

Observe that $v'_{n+1} = [1\ 1\ \cdots\ 1]$ and $2 \in (\mathbb{Z}/p\mathbb{Z})^\times$. For $1 \le i \le n$, if $v'_{ij} = 1$ (resp., -1), then $v_{i\ell-j} = -1$ (resp., 1). Thus, we can write v'_i as a linear combination of the row vectors of the above row echelon form (4.2), and hence, the claim is proved. By the above claim, $\operatorname{rank}(N'_\ell) = n+1$ if and only if $\det([n_{ij}]_{1\le i,j\le n+1}) \not\equiv 0 \pmod p$. Since

$$[-n_{1j} + n_{nj} + n_{n+1j}]_{1\le j\le n+1} = [0\ 0\ \cdots\ 0\ 1],$$

we derive

$$\det\big([n_{ij}]_{1\le i,j\le n+1}\big) = \det(N_\ell).$$

This completes the proof. □

THEOREM 4.5

Let ℓ and p be odd primes, and put $n = (\ell-1)/2$. Further, let $M_\ell(p)$ and N_ℓ be as above. If $p \nmid \ell h_\ell^+ n$, then for every $\mu \in \mathbb{Z}_{>0}$ we deduce

$$\operatorname{Gal}(K_\mu/k_\mu) \cong (\mathbb{Z}/p\mathbb{Z})^{\operatorname{rank}(M_\ell(p))}.$$

If $p \nmid \det(N_\ell)$, then we obtain

$$\operatorname{Gal}(K_\mu/k_\mu) \cong (\mathbb{Z}/p\mathbb{Z})^{n+1}.$$

Proof

By (4.1) it suffices to show that the dimension of $\langle \eta_{\mu,1}S_{\mu+1}, \eta_{\mu,2}S_{\mu+1}, \dots, \eta_{\mu,n+1}S_{\mu+1}\rangle$ in $S_\mu/S_{\mu+1}$ is equal to the dimension of $\langle \eta_{\mu,1}H_\mu, \eta_{\mu,2}H_\mu, \dots, \eta_{\mu,n+1}H_\mu\rangle$ in S_μ/H_μ. If $n = 1$, then $H_\mu = S_{\mu+1}$ by Lemma 4.3; hence, we are done in this case. Thus, we may assume $n \ge 2$. It is well known that $\mathbb{Z}[\zeta+\zeta^{-1}]$ is the ring of integers of the maximal real subfield $\mathbb{Q}(\zeta+\zeta^{-1})$ of k and $[\mathbb{Q}(\zeta+\zeta^{-1}) : \mathbb{Q}] = n$ (see [16, Theorem 4]). Therefore, if $uS_{\mu+1} \in H_\mu/S_{\mu+1}$, then by Lemma 4.3 we can write

$$u = 1 + 2p^\mu\big(a_0 + a_1(\zeta+\zeta^{-1}) + a_2(\zeta+\zeta^{-1})^2 + \cdots + a_{n-1}(\zeta+\zeta^{-1})^{n-1}\big) \in S_\mu \cap E$$

for some $a_i \in \mathbb{Z}$ with $0 \le i \le n-1$. If $p \mid a_i$ for $1 \le i \le n-1$, then

$$\begin{aligned} N_{\mathbb{Q}(\zeta+\zeta^{-1})/\mathbb{Q}}(u) &\equiv 1 + 2p^\mu n a_0 \pmod{2p^{\mu+1}} \\ &\equiv 1 \pmod{2p^{\mu+1}}. \end{aligned}$$

Since $p \nmid n$, we have $p \mid a_0$ and so $u \in S_{\mu+1}$.

Now, we set

$$\begin{aligned} b &= a_0 + a_1(\zeta+\zeta^{-1}) + a_2(\zeta+\zeta^{-1})^2 + \cdots + a_{n-1}(\zeta+\zeta^{-1})^{n-1} \\ &= b_0 + b_1\zeta + b_2\zeta^2 + \cdots + b_n\zeta^n + b_n\zeta^{-n} + b_{n-1}\zeta^{-(n-1)} + \cdots + b_1\zeta^{-1}, \end{aligned}$$

where $b_i \in \mathbb{Z}$ for $0 \le i \le n$. Observe that $b_n = 0$, $b_{n-1} = a_{n-1}$, and $b_{n-2} = a_{n-2}$. Consider the following matrix:

$$\mathbf{M} = \begin{bmatrix} 1 & & & & & & & & -1 \\ & 1 & & & & & & -1 & \\ & & \ddots & & & & \iddots & & \\ & & & 1 & -1 & & & & \\ & & & & 1 & 1 & \cdots & 1 & \\ b_1 - b_0 & b_2 - b_0 & \cdots & b_n - b_0 & b_n - b_0 & \cdots & b_2 - b_0 & b_1 - b_0 & \end{bmatrix}$$

$$\in M_{(n+2)\times 2n}(\mathbb{Z}/p\mathbb{Z}).$$

The last row of $\mathbf{M}$ is induced from the coefficients of ζ^j for $1 \le j \le 2n$ in b. So, $\mathbf{M}$ is row equivalent to

$$\mathbf{M} \sim \begin{bmatrix} 1 & & & & & & & -1 \\ & 1 & & & & & -1 & \\ & & \ddots & & & \iddots & & \\ & & & 1 & -1 & & & \\ & & & & 1 & 1 & \cdots & 1 \\ 0 & 0 & \cdots & 0 & 2(b_n - b_0) & 2(b_{n-1} - b_0) & \cdots & 2(b_1 - b_0) \end{bmatrix}$$

$$\sim \begin{bmatrix} 1 & & & & & & & -1 \\ & 1 & & & & & -1 & \\ & & \ddots & & & \iddots & & \\ & & & 1 & -1 & & & \\ & & & & 1 & 1 & \cdots & 1 \\ 0 & 0 & \cdots & 0 & 0 & 2b_{n-1} & \cdots & 2b_1 \end{bmatrix} \quad \text{because } b_n = 0.$$

Here we claim that if $u \notin S_{\mu+1}$, then the rank of $\mathbf{M}$ is $n+2$. Indeed, if $p \nmid a_{n-1}$ or $p \nmid a_{n-2}$, then we are done. Otherwise, we get

$$b_{n-3} \equiv a_{n-3} \pmod{p},$$
$$b_{n-4} \equiv a_{n-4} \pmod{p}.$$

Hence, by induction we ensure that the rank of $\mathbf{M}$ is $n+1$ if and only if $p \mid a_i$ for all $1 \le i \le n-1$. Since $u \notin S_{\mu+1}$, we obtain $p \nmid a_i$ for some $1 \le i \le n-1$, and the claim is proved. In the proof of Lemma 4.4 we already showed that every row vector of $M_\ell(p)$ can be written as a linear combination of the row vectors of the matrix (4.2). Therefore, if $u \notin S_{\mu+1}$, then by the above claim for each $1 \le i \le n+1$ the images of $\eta_{\mu,i}$ and u in $S_\mu/S_{\mu+1}$ are linearly independent, as desired. Furthermore, if $p \nmid \det(N_\ell)$, then by Lemma 4.4 we obtain $\operatorname{rank}(M_\ell(p)) = n+1$. □

COROLLARY 4.6

Suppose that $p \nmid \ell h_\ell^+ n$. Then K_μ becomes the ray class field $k_{\mu+1}$ for all $\mu \in \mathbb{Z}_{>0}$ if and only if $\dim_{\mathbb{Z}/p\mathbb{Z}}(H_1/S_2) = n-1$ and $p \nmid \det(N_\ell)$.

Proof

Suppose that $\dim_{\mathbb{Z}/p\mathbb{Z}}(H_1/S_2) = n-1$ and $p \nmid \det(N_\ell)$. We claim that $\dim_{\mathbb{Z}/p\mathbb{Z}}(H_\mu/S_{\mu+1}) = n-1$ for all $\mu \in \mathbb{Z}_{>0}$. Indeed, let $\varepsilon_1, \varepsilon_2, \dots, \varepsilon_{n-1}$ be elements of $S_1 \cap E$ whose images form a basis for H_1/S_2. Since $\varepsilon_i^p \in H_2 - S_3$ for all i, the images $\varepsilon_1^p, \varepsilon_2^p, \dots, \varepsilon_{n-1}^p$ turn out to be a basis for H_2/S_3. By induction, the claim is proved. By Theorem 4.5 and the assumptions, we deduce

$$\big|\mathrm{Gal}(K_\mu/k_\mu)\big| = \big|\widetilde{\varphi_\mu^*}(S_\mu/H_\mu)\big| = p^{n+1},$$

$$\big|\mathrm{Gal}(k_{\mu+1}/k_\mu)\big| = |S_\mu/H_\mu| = \frac{|S_\mu/S_{\mu+1}|}{|H_\mu/S_{\mu+1}|} = p^{n+1}.$$

Therefore, $K_\mu = k_{\mu+1}$ because $K_\mu \subset k_{\mu+1}$.

Conversely, suppose that $K_\mu = k_{\mu+1}$ for all $\mu \in \mathbb{Z}_{>0}$. It follows from the proof of Lemma 4.3 that $|H_\mu/S_{\mu+1}| \le p^{n-1}$, and so $|\mathrm{Gal}(k_{\mu+1}/k_\mu)| \ge p^{n+1}$. On the other hand, $|\mathrm{Gal}(K_\mu/k_\mu)| \le p^{n+1}$ by the formula (4.1). Since $K_\mu = k_{\mu+1}$, we have $\dim_{\mathbb{Z}/p\mathbb{Z}}(H_1/S_2) = n-1$ and $|\mathrm{Gal}(K_\mu/k_\mu)| = p^{n+1}$; hence $p \nmid \det(N_\ell)$ by Lemma 4.4 and Theorem 4.5. □

REMARK 4.7

(i) We are able to show that $\det(N_\ell) \neq 0$ for $\ell \le 10000$ with the aid of Maple software, from which we conjecture that $\det(N_\ell) \neq 0$ holds for all odd primes ℓ.

(ii) Let $\xi_a = \zeta_{2\ell}^{1-a}(1-\zeta^a)/(1-\zeta) \in \mathbb{R}$ for $1 < a < \ell/2$. When $\ell = 5$, we obtain

$$\xi_2^{48} \equiv 1 \pmod{14}$$
$$\not\equiv 1 \pmod{98}.$$

Thus, $\dim_{\mathbb{Z}/7\mathbb{Z}}(H_1/S_2) = 1$, and Corollary 4.6 is true for $p = 7$. In a similar way, we can show that $\dim_{\mathbb{Z}/p\mathbb{Z}}(H_1/S_2) = 1$ holds for all odd primes $p \le 101$ except $p = 3$. When $\ell = 7$, we see that $\dim_{\mathbb{Z}/p\mathbb{Z}}(H_1/S_2) = 2$ for all odd primes $p \le 101$. So, we also conjecture that, for each odd prime ℓ, $\dim_{\mathbb{Z}/p\mathbb{Z}}(H_1/S_2) = n-1$ holds for almost all odd primes p. If the above two conjectures are true, then we have the isomorphism

$$\mathrm{Gal}(k_{\mu+1}/k_\mu) \cong (\mathbb{Z}/p\mathbb{Z})^{n+1}$$

for each odd prime ℓ and almost all odd primes p.

(iii) Table 1 lists the generators of H_1/S_2 for $\ell = 5, 7$.

5. Theta functions

In this section, we shall provide necessary fundamental transformation formulas of theta functions and describe the action of $G_{\mathbb{A}+}$ on the quotient of two theta constants.

Let n be a positive integer, and let $u \in \mathbb{C}^n$, $z \in \mathbb{H}_n$, and $r, s \in \mathbb{R}^n$. We define a (classical) *theta function* by

$$\Theta(u, z; r, s) = \sum_{x \in \mathbb{Z}^n} e\Big(\frac{1}{2} \cdot {}^t(x+r)z(x+r) + {}^t(x+r)(u+s)\Big).$$

Table 1

p	generators of H_1/S_2	
	$\ell=5$	$\ell=7$
3	1	ξ_2^{182},ξ_3^{182}
5	ξ_2^{60}	ξ_2^{868},ξ_3^{868}
7	ξ_2^{48}	ξ_2^{42},ξ_3^{42}
11	ξ_2^{30}	$\xi_2^{1330},\xi_3^{1330}$
13	ξ_2^{84}	ξ_2^{84},ξ_3^{84}
17	ξ_2^{72}	$\xi_2^{17192},\xi_3^{34384}$
19	ξ_2^{18}	$\xi_2^{16002},\xi_3^{16002}$
23	ξ_2^{528}	$\xi_2^{12166},\xi_3^{12166}$
29	ξ_2^{848}	ξ_2^{28},ξ_3^{28}
31	ξ_2^{30}	$\xi_2^{69510},\xi_3^{69510}$
37	ξ_2^{684}	$\xi_2^{16884},\xi_3^{16884}$
41	ξ_2^{120}	ξ_2^{280},ξ_3^{280}
43	ξ_2^{1848}	ξ_2^{42},ξ_3^{42}

p	generators of H_1/S_2	
	$\ell=5$	$\ell=7$
47	ξ_2^{2208}	$\xi_2^{726754},\xi_3^{726754}$
53	ξ_2^{1404}	$\xi_2^{148876},\xi_3^{148876}$
59	ξ_2^{174}	$\xi_2^{1437646},\xi_3^{1437646}$
61	ξ_2^{60}	$\xi_2^{40740},\xi_3^{40740}$
67	ξ_2^{4488}	$\xi_2^{100254},\xi_3^{100254}$
71	ξ_2^{210}	ξ_2^{70},ξ_3^{70}
73	ξ_2^{1332}	$\xi_2^{226926},\xi_3^{453852}$
79	ξ_2^{78}	$\xi_2^{164346},\xi_3^{164346}$
83	ξ_2^{6888}	ξ_2^{574},ξ_3^{574}
89	ξ_2^{132}	$\xi_2^{1233694},\xi_3^{4934776}$
97	ξ_2^{2352}	ξ_2^{672},ξ_3^{672}
101	ξ_2^{300}	$\xi_2^{7212100},\xi_3^{7212100}$

PROPOSITION 5.1

Let $r,s\in\mathbb{R}^n$ and $a,b\in\mathbb{Z}^n$. We have

(i) $\Theta(-u,z;-r,-s)=\Theta(u,z;r,s)$,
(ii) $\Theta(u,z;r+a,s+b)=e({}^trb)\Theta(u,z;r,s)$.

Proof
See [26, p. 676, (13)]. □

For a square matrix S, by $\{S\}$ we mean the column vector whose components are the diagonal entries of S.

PROPOSITION 5.2

For every $\gamma=\left[\begin{smallmatrix}A & B\\ C & D\end{smallmatrix}\right]\in\Gamma(1)$ such that $\{{}^tAC\},\{{}^tBD\}\in 2\mathbb{Z}^n$, we get the transformation formula

$$\begin{aligned}&\Theta\big({}^t(Cz+D)^{-1}u,\gamma(z);r,s\big)\\ &\quad=\lambda_\gamma e\Big(\frac{{}^trs-{}^tr's'}{2}\Big)\det(Cz+D)^{1/2}e\Big(\frac{1}{2}\cdot{}^tu(Cz+D)^{-1}cu\Big)\\ &\qquad\times\Theta(u,z;r',s'),\end{aligned}$$

where λ_γ is a constant of absolute value 1 depending only on γ and the choice of the branch of $\det(Cz+D)^{1/2}$, and

$$\begin{bmatrix}r'\\ s'\end{bmatrix}={}^t\gamma\begin{bmatrix}r\\ s\end{bmatrix}.$$

In particular, $\lambda_\gamma^4=1$ for $\gamma\in\Gamma(2)$.

Proof
See [26, Propositions 1.3 and 1.4]. □

Here, the functions $\Theta(0,z;r,s)$ are called *theta constants*, and these are holomorphic on $\mathbb{H}_n$ as functions in z (see [26, Proposition 1.6]).

PROPOSITION 5.3
Suppose that r, s belong to $\mathbb{Q}^n$. Then the theta constant $\Theta(0,z;r,s)$ represents the zero function if and only if $r,s\in(1/2)\mathbb{Z}^n$ and $e(2\cdot {}^t rs)=-1$.

Proof
See [11, Theorem 2]. □

Let

$$\Phi_{(r,s)}(z)=\frac{\Theta(0,z;r,s)}{\Theta(0,z;0,0)}.$$

Note that the poles of $\Phi_{(r,s)}(z)$ are exactly the zeros of $\Theta(0,z;0,0)=\sum_{x\in\mathbb{Z}^n} e(\frac{1}{2}{}^t xzx)$. When $n=1$, $\Theta(0,z;0,0)$ has no zero on $\mathbb{H}_1$ by Jacobi's triple product identity (see [1, Theorem 14.6]).

LEMMA 5.4
For $r,s\in\mathbb{R}^n$ and $a,b\in\mathbb{Z}^n$, we obtain that

(i) $\Phi_{(-r,-s)}(z)=\Phi_{(r,s)}(z)$,
(ii) $\Phi_{(r+a,s+b)}(z)=e({}^t rb)\Phi_{(r,s)}(z)$,
(iii) *if* $\gamma=\left[\begin{smallmatrix}A & B\\ C & D\end{smallmatrix}\right]\in\Gamma(1)$ *such that* $\{{}^t AC\},\{{}^t BD\}\in 2\mathbb{Z}^n$, *then we obtain*

$$\Phi_{(r,s)}\big(\gamma(z)\big)=e\Big(\frac{{}^t rs-{}^t r's'}{2}\Big)\Phi_{(r',s')}(z),$$

where

$$\begin{bmatrix}r'\\ s'\end{bmatrix}={}^t\gamma\begin{bmatrix}r\\ s\end{bmatrix}.$$

Proof
It is immediate from Propositions 5.1 and 5.2. □

PROPOSITION 5.5
Let m be a positive integer, and let $r,s\in(1/m)\mathbb{Z}^n$. Then $\Phi_{(r,s)}(z)$ belongs to $\mathcal{F}_{2m^2}$. Moreover, if x is an element of Δ such that

$$x_q\equiv\begin{bmatrix}1_n & 0\\ 0 & t1_n\end{bmatrix}\pmod{2m^2M_{2n}(\mathbb{Z}_q)}$$

for all rational primes q and a positive integer t, then

$$\Phi_{(r,s)}(z)^x=\Phi_{(r,ts)}(z).$$

Proof
See [26, Proposition 1.7]. □

COROLLARY 5.6
For $m \in \mathbb{Z}_{>0}$ and $r, s \in (1/m)\mathbb{Z}^n$, let

$$y = \beta \begin{bmatrix} 1_n & 0 \\ 0 & x \cdot 1_n \end{bmatrix} \alpha \in G_{\mathbb{A}+}$$

with $\beta \in R_{2m^2}$, $x \in \prod_q \mathbb{Z}_q^\times$, and $\alpha \in G_{\mathbb{Q}+}$. Then

$$(\Phi_{(r,s)})^y(z) = \Phi_{(r,ts)}\big(\alpha(z)\big),$$

where t is a positive integer such that $t \equiv x_q \pmod{2m^2\mathbb{Z}_q}$ for all rational primes q.

Proof
This can be proved by Propositions 2.2 and 5.5. □

6. Construction of class fields

We use the same notation as in Section 4. Let $k = \mathbb{Q}(\zeta)$ with $\zeta = \zeta_\ell$, and let $n = (\ell - 1)/2$ so that $2n = [k : \mathbb{Q}]$. Let $v : k \to \mathbb{C}^n$ be the map given by

$$v(x) = \begin{bmatrix} x^{\varphi_1} \\ \vdots \\ x^{\varphi_n} \end{bmatrix},$$

let $L = v(\mathcal{O}_k)$ be a lattice in $\mathbb{C}^n$, and let $\rho = (\zeta - \zeta^{-1})/\ell \in k$. Then ρ satisfies conditions (i)–(iii) in Section 3. We have an $\mathbb{R}$-bilinear form $E : \mathbb{C}^n \times \mathbb{C}^n \to \mathbb{R}$ defined by

$$E(z, w) = \sum_{i=1}^{n} \rho^{\varphi_i}(z_i\overline{w_i} - \overline{z_i}w_i) \quad \text{for } z = \begin{bmatrix} z_1 \\ \vdots \\ z_n \end{bmatrix}, w = \begin{bmatrix} w_1 \\ \vdots \\ w_n \end{bmatrix},$$

which induces a nondegenerate Riemann form on $\mathbb{C}^n/L$. Let

$$e_i = \begin{cases} \zeta^{2i} & \text{for } 1 \le i \le n, \\ \sum_{j=1}^{i-n} \zeta^{2j-1} & \text{for } n+1 \le i \le 2n. \end{cases}$$

Since $\{e_1, e_2, \ldots, e_{2n}\}$ is a free $\mathbb{Z}$-basis of $\mathcal{O}_k$, $\{v(e_1), v(e_2), \ldots, v(e_{2n})\}$ is a free $\mathbb{Z}$-basis of the lattice L, and we get

$$\big[E\big(v(e_i), v(e_j)\big)\big]_{1 \le i,j \le 2n} = J.$$

Now, let

$$\Omega = \big[v(e_1)\ v(e_2)\ \cdots\ v(e_{2n})\big] \in M_{n \times 2n}(\mathbb{C}).$$

Then Ω satisfies

$$L = \left\{ \Omega \begin{bmatrix} a \\ b \end{bmatrix} \,\middle|\, a, b \in \mathbb{Z}^n \right\},$$

$$E(\Omega x, \Omega y) = {}^t x J y \quad \text{for } x, y \in \mathbb{R}^{2n},$$

because E is $\mathbb{R}$-bilinear. Thus, $\delta = 1$ and $\epsilon = 1_n$ in Section 3. Write $\Omega = [\Omega_1\ \Omega_2]$ with $\Omega_1, \Omega_2 \in M_n(\mathbb{C})$, and put $z_\ell = \Omega_2^{-1}\Omega_1 \in \mathbb{H}_n$. We define a ring monomorphism h of $k_{\mathbb{A}}$ into $M_{2n}(\mathbb{Q}_{\mathbb{A}})$ as in Section 3. Then z_ℓ is the CM-point of $\mathbb{H}_n$ induced from h corresponding to the polarized abelian variety $(\mathbb{C}^n/L, E)$.

Let p be an odd prime, and let $r, s \in \mathbb{Q}^n$. We denote by $\mathbf{h}$ the set of all non-Archimedean primes of k and by $\mathbf{a}$ the set of all archimedean primes of k. For given $\omega \in \mathcal{O}_k$ prime to $2p$, we set

$$\widetilde{\omega} = \prod_{\substack{v \in \mathbf{h} \\ v \mid 2p}} (\omega^{-1})_v \times \prod_{\substack{v \in \mathbf{h} \\ v \nmid 2p}} 1_v \times \prod_{v \in \mathbf{a}} 1_v \in k_{\mathbb{A}}^{\times}.$$

Here x_v is the v-component of $x \in k_{\mathbb{A}}^{\times}$. If $\Phi_{(r,s)}$ is finite at z_ℓ, then by Proposition 3.2 and [15, Chapter 8, Section 4], we have

$$\Phi_{(r,s)}(z_\ell)^{\left(\frac{k'/k}{(\omega)}\right)} = \Phi_{(r,s)}(z_\ell)^{[\widetilde{\omega},k]} = \left(\Phi_{(r,s)}\right)^{h(\varphi^*(\widetilde{\omega}^{-1}))}(z_\ell) \quad \text{for } \omega \in \mathcal{O}_k,$$

where k' is a finite abelian extension of k containing $\Phi_{(r,s)}(z_\ell)$.

LEMMA 6.1

Let p be an odd prime, let $\mu \in \mathbb{Z}_{>0}$, let $r, s \in (1/p^\mu)\mathbb{Z}^n$, and let z_ℓ be as above. Assume that z_ℓ is not a zero of $\Theta(0, z; 0, 0)$. If $p \nmid \ell h_\ell^+ n$, then $\Phi_{(r,s)}(z_\ell)^{p^\alpha} \in K_{2\mu-1-\alpha}$ for $\alpha = 0, 1, \ldots, \mu$.

Proof

By Proposition 5.5 and [26, p. 682], $\Phi_{(r,s)}(z)$ belongs to $\widetilde{\mathcal{F}_{2p^{2\mu}}}$ as a function, so it is $R_{2p^{2\mu}}$-invariant. Let $\omega H_{2\mu-1-\alpha}$ belong to $\ker(\widetilde{\varphi^*_{2\mu-1-\alpha}})$ such that $\varphi^*(\omega) \in H_{2\mu-1-\alpha}$. Since $p \nmid \ell h_\ell^+ n$, it follows from the proof of Theorem 4.5 that $(\varphi^*(S_{2\mu-1-\alpha}) \cap H_{2\mu-1-\alpha})/S_{2\mu-\alpha} = \{0\}$. Hence, $\varphi^*(\omega) \in S_{2\mu-\alpha}$. Write $\varphi^*(\omega) = 1 + 2p^{2\mu-\alpha}\omega_0$ with $\omega_0 \in \mathcal{O}_k$. Then it suffices to show that $(\Phi_{(r,s)}(z_\ell)^{p^\alpha})^{\left(\frac{k'/k}{(\omega)}\right)} = \Phi_{(r,s)}(z_\ell)^{p^\alpha}$, where k' is a finite abelian extension of k containing $\Phi_{(r,s)}(z_\ell)$. By the strong approximation theorem for $\mathrm{Sp}(n)$ there exists a matrix $\beta \in \Gamma(1)$ such that

$$h\big(\varphi^*(\omega)\big) \equiv \begin{bmatrix} 1_n & 0 \\ 0 & v \cdot 1_n \end{bmatrix} \beta \pmod{2p^{2\mu}},$$

where $v := \nu(h(\varphi^*(\omega))) = N_{k/\mathbb{Q}}(\omega) = \varphi^*(\omega) \cdot \overline{\varphi^*(\omega)} = 1 + 2p^{2\mu-\alpha}v_0$ for some $v_0 \in \mathbb{Z}$. In fact, β belongs to $\Gamma(2)$ because $h(\varphi^*(\omega)) \equiv 1_{2n} \pmod 2$ and $v \equiv 1 \pmod 2$. Thus, for all rational primes q we obtain

$$h\big(\varphi^*(\widetilde{\omega}^{-1})\big)_q \equiv \begin{bmatrix} 1_n & 0 \\ 0 & v \cdot 1_n \end{bmatrix} \beta \pmod{2p^{2\mu} M_{2n}(\mathbb{Z}_q)}.$$

By Lemma 5.4 and Corollary 5.6 we get that

$$\begin{aligned}(\Phi_{(r,s)})^{h(\varphi^*(\tilde{\omega}^{-1}))}(z_\ell) &= \Phi_{(r,vs)}(\beta z_\ell)\\ &= e\Big(\frac{{}^t rvs - {}^t r's'}{2}\Big)\Phi_{(r',s')}(z_\ell),\end{aligned}$$

where

$$\begin{aligned}\begin{bmatrix} r' \\ s' \end{bmatrix} = {}^t\beta \begin{bmatrix} r \\ vs \end{bmatrix} &\equiv {}^t h\big(\varphi^*(\omega)\big) \begin{bmatrix} r \\ s \end{bmatrix} \pmod{2p^{2\mu}}\\ &\equiv \begin{bmatrix} r \\ s \end{bmatrix} + 2p^{2\mu-\alpha}\cdot {}^t h(\omega_0) \begin{bmatrix} r \\ s \end{bmatrix} \pmod{2p^{2\mu}}.\end{aligned}$$

Let $a, b \in 2p^{\mu-\alpha}\mathbb{Z}^n \subset 2\mathbb{Z}^n$ such that $\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right] = 2p^{2\mu-\alpha}\cdot {}^t h(\omega_0)\left[\begin{smallmatrix} r \\ s \end{smallmatrix}\right]$. Then we derive by Lemma 5.4 and Proposition 3.2 that

$$\begin{aligned}\big(\Phi_{(r,s)}(z_\ell)^{p^\alpha}\big)^{\left(\frac{k'/k}{(\omega)}\right)} &= \big(\Phi_{(r,s)}{}^{h(\varphi^*(\tilde{\omega}^{-1}))}(z_\ell)\big)^{p^\alpha}\\ &= \Big(e\Big(\frac{{}^t rvs - {}^t(r+a)(s+b)}{2}\Big)e({}^t rb)\Phi_{(r,s)}(z_\ell)\Big)^{p^\alpha}\\ &= e(p^{2\mu}v_0\cdot {}^t rs)e\Big(p^\alpha\cdot\frac{{}^t rb - {}^t as}{2}\Big)\Phi_{(r,s)}(z_\ell)^{p^\alpha}\\ &= \Phi_{(r,s)}(z_\ell)^{p^\alpha}.\end{aligned}$$

□

Let $\mu \in \mathbb{Z}_{>0}$. Assume that $r, s \in (1/p^\mu)\mathbb{Z}^n$ and that z_ℓ is not a zero of $\Theta(0, z; 0, 0)$. Consider the matrices $h(\varphi^*(\omega_{2\mu-1-\alpha,j}))$ for $1 \le j \le n+1$ and $0 \le \alpha \le \mu-1$. Then we have

$$\begin{aligned}h\big(\varphi^*(\omega_{2\mu-1-\alpha,j})\big) &= h\big(1 + 2p^{2\mu-1-\alpha}\varphi^+(\zeta^j) + 2p^{2\mu-\alpha}\omega_0\big)\\ &= 1_{2n} + 2p^{2\mu-1-\alpha}h\big(\varphi^+(\zeta^j)\big) + 2p^{2\mu-\alpha}h(\omega_0)\end{aligned}$$

for some $\omega_0 \in \mathcal{O}_k$. Also, we can deduce without difficulty

$$h(\zeta) = \left[\begin{array}{ccccc|ccccc} 0 & 0 & \cdots & \cdots & 0 & -1 & 1 & & & \\ \vdots & \vdots & & & \vdots & & -1 & 1 & & \\ \vdots & \vdots & & & \vdots & & & \ddots & \ddots & \\ 0 & 0 & \cdots & \cdots & 0 & & & & -1 & 1 \\ -1 & -1 & \cdots & \cdots & -1 & & & & & -1 \\ \hline 1 & & & & & 0 & 0 & \cdots & \cdots & 0 \\ 1 & 1 & & & & \vdots & \vdots & & & \vdots \\ 1 & 1 & 1 & & & \vdots & \vdots & & & \vdots \\ \vdots & \vdots & & \ddots & & \vdots & \vdots & & & \vdots \\ 1 & 1 & 1 & \cdots & 1 & 0 & 0 & \cdots & \cdots & 0 \end{array}\right].$$

Now, again by the strong approximation theorem for $\mathrm{Sp}(n)$ there exists a matrix $\beta_{2\mu-1-\alpha,j}$ in $\Gamma(1)$ such that

$$h\big(\varphi^*(\omega_{2\mu-1-\alpha,j})\big) \equiv \begin{bmatrix} 1_n & 0 \\ 0 & v_{2\mu-1-\alpha,j}\cdot 1_n \end{bmatrix} \beta_{2\mu-1-\alpha,j} \pmod{2p^{2\mu}},$$

where $v_{2\mu-1-\alpha,j} := \nu(h(\varphi^*(\omega_{2\mu-1-\alpha,j}))) = N_{k/\mathbb{Q}}(\omega_{2\mu-1-\alpha,j}) = 1 - 2p^{2\mu-1-\alpha} + 2p^{2\mu-\alpha}v_j$ for some $v_j \in \mathbb{Z}$. As a matter of fact, $\beta_{2\mu-1-\alpha,j}$ belongs to $\Gamma(2)$ because $h(\varphi^*(\omega_{2\mu-1-\alpha,j})) \equiv 1_{2n} \pmod 2$ and $v_{2\mu-1-\alpha,j} \equiv 1 \pmod 2$. For all rational primes q we obtain

$$h\big(\varphi^*(\widetilde{\omega}_{2\mu-1-\alpha,j}^{-1})\big)_q \equiv \begin{bmatrix} 1_n & 0 \\ 0 & v_{2\mu-1-\alpha,j}\cdot 1_n \end{bmatrix} \beta_{2\mu-1-\alpha,j} \pmod{2p^{2\mu}M_{2n}(\mathbb{Z}_q)}.$$

By Lemma 5.4 and Corollary 5.6 we obtain

$$\begin{aligned}\Phi_{(r,s)}{}^{h(\varphi^*(\widetilde{\omega}_{2\mu-1-\alpha,j}^{-1}))}(z_\ell) &= \Phi_{(r,v_{2\mu-1-\alpha,j}s)}\big(\beta_{2\mu-1-\alpha,j}(z_\ell)\big)\\ &= e\Big(\frac{{}^t r v_{2\mu-1-\alpha,j}s - {}^t r's'}{2}\Big)\Phi_{(r',s')}(z_\ell),\end{aligned}$$

where

$$\begin{aligned}\begin{bmatrix} r' \\ s' \end{bmatrix} &= {}^t\beta_{2\mu-1-\alpha,j}\begin{bmatrix} r \\ v_{2\mu-1-\alpha,j}s \end{bmatrix}\\ &\equiv {}^t h\big(\varphi^*(\omega_{2\mu-1-\alpha,j})\big)\begin{bmatrix} r \\ s \end{bmatrix} \pmod{2p^{2\mu}}\\ &\equiv \begin{bmatrix} r \\ s \end{bmatrix} + 2p^{2\mu-1-\alpha}\cdot {}^t h\big(\varphi^+(\zeta^j)\big)\begin{bmatrix} r \\ s \end{bmatrix} + 2p^{2\mu-\alpha}\cdot {}^t h(\omega_0)\begin{bmatrix} r \\ s \end{bmatrix} \pmod{2p^{2\mu}}.\end{aligned}$$

For each j, let $a_{2\mu-1-\alpha,j}, b_{2\mu-1-\alpha,j} \in 2p^{\mu-1-\alpha}\mathbb{Z}^n \subset 2\mathbb{Z}^n$ such that

$$\begin{bmatrix} a_{2\mu-1-\alpha,j} \\ b_{2\mu-1-\alpha,j} \end{bmatrix} = 2p^{2\mu-1-\alpha}\cdot {}^t h\big(\varphi^+(\zeta^j)\big)\begin{bmatrix} r \\ s \end{bmatrix}.$$

Let $c, d \in 2p^{\mu-\alpha}\mathbb{Z}^n \subset 2\mathbb{Z}^n$ for which $\left[\begin{smallmatrix} c \\ d \end{smallmatrix}\right] = 2p^{2\mu-\alpha}\cdot {}^t h(\omega_0)\left[\begin{smallmatrix} r \\ s \end{smallmatrix}\right]$. Then by Lemma 5.4 and Proposition 3.2 we derive that

$$\begin{aligned}&\big(\Phi_{(r,s)}(z_\ell)^{p^\alpha}\big)^{\left(\frac{K_{2\mu-1-\alpha}/k}{(\omega_{2\mu-1-\alpha,j})}\right)}\\ &\quad= \big(\Phi_{(r,s)}{}^{h(\varphi^*(\widetilde{\omega}_{2\mu-1-\alpha,j}^{-1}))}(z_\ell)\big)^{p^\alpha}\\ &\quad= e\Big(p^\alpha\frac{{}^t r v_{2\mu-1-\alpha,j}s - {}^t(r+a_{2\mu-1-\alpha,j}+c)(s+b_{2\mu-1-\alpha,j}+d)}{2}\Big)\\ &\qquad\times e\big(p^\alpha\cdot {}^t r(b_{2\mu-1-\alpha,j}+d)\big)\Phi_{(r,s)}(z_\ell)^{p^\alpha} \qquad (6.1)\\ &\quad= e(-p^{2\mu-1}\cdot {}^t rs)e\Big(p^\alpha\frac{{}^t r b_{2\mu-1-\alpha,j} - {}^t a_{2\mu-1-\alpha,j}s}{2}\Big)\Phi_{(r,s)}(z_\ell)^{p^\alpha}\\ &\quad= \underbrace{e(-p^{2\mu-1}\cdot {}^t rs)e\Big(\frac{{}^t r b_{2\mu-1,j} - {}^t a_{2\mu-1,j}s}{2}\Big)}_{p\text{th root of unity}}\Phi_{(r,s)}(z_\ell)^{p^\alpha}.\end{aligned}$$

For given $r_i, s_i \in \mathbb{Z}^n$ with $1 \le i \le n+1$, let $\mathbf{r} = [r_i]_{1\le i\le n+1}$ and $\mathbf{s} = [s_i]_{1\le i\le n+1}$. We set $\Phi_{[\mathbf{r},\mathbf{s};\mu,i]}(z)_p = \Phi_{(r_i/p^\mu, s_i/p^\mu)}(z)$ for each $\mu \in \mathbb{Z}_{>0}$.

LEMMA 6.2

Let $\mathbf{r} = [r_i]_{1\le i\le n+1}$ and $\mathbf{s} = [s_i]_{1\le i\le n+1}$ for given $r_i, s_i \in \mathbb{Z}^n$. Then for each $1 \le i, j \le n+1$, there exists an integer c_{ij} such that

$$\Phi_{[\mathbf{r},\mathbf{s};1,i]}(z_\ell)_p^{\left(\frac{K_1/k}{(\omega_{1,j})}\right)} = \zeta_p^{c_{ij}}\Phi_{[\mathbf{r},\mathbf{s};1,i]}(z_\ell)_p$$

for all odd primes p.

Proof

Substituting $r = r_i/p$ and $s = s_i/p$ into the formula (6.1) we get

$$\begin{aligned}\Phi_{[\mathbf{r},\mathbf{s};1,i]}(z_\ell)_p^{\left(\frac{K_1/k}{(\omega_{1,j})}\right)} &= e\Big(-\frac{{}^t r_i s_i}{p}\Big)e\Big(\frac{{}^t r_i b_{1,j} - {}^t a_{1,j} s_i}{2p}\Big)\Phi_{[\mathbf{r},\mathbf{s};1,i]}(z_\ell)_p\\ &= \zeta_p^{-{}^t r_i s_i + ({}^t r_i b_{1,j} - {}^t a_{1,j} s_i)/2}\Phi_{[\mathbf{r},\mathbf{s};1,i]}(z_\ell)_p,\end{aligned}$$

where $a_{1,j}, b_{1,j} \in 2\mathbb{Z}^n$ such that $\left[\begin{smallmatrix} a_{1,j} \\ b_{1,j}\end{smallmatrix}\right] = 2\cdot {}^t h(\varphi^+(\zeta^j))\left[\begin{smallmatrix} r_i \\ s_i\end{smallmatrix}\right]$. Hence,

$$c_{ij} := -{}^t r_i s_i + \frac{1}{2}({}^t r_i b_{1,j} - {}^t a_{1,j} s_i)$$

is an integer which does not depend on p. □

We put $A_\ell(\mathbf{r},\mathbf{s}) = [c_{ij}]_{1\le i,j\le n+1} \in M_{n+1}(\mathbb{Z})$, where c_{ij} is an integer satisfying

$$\Phi_{[\mathbf{r},\mathbf{s};1,i]}(z_\ell)_p^{\left(\frac{K_1/k}{(\omega_{1,j})}\right)} = \zeta_p^{c_{ij}}\Phi_{[\mathbf{r},\mathbf{s};1,i]}(z_\ell)_p$$

for all odd primes p. Note that $A_\ell(\mathbf{r},\mathbf{s})$ does not depend on p by Lemma 6.2.

Now, in order to construct a primitive generator of K_μ over k_μ, we need the following lemma.

LEMMA 6.3

Let L be an abelian extension of a number field F. Suppose that $L = F(\alpha,\beta)$ for some $\alpha, \beta \in L$. Let a, b be any nonzero elements of F, and let $\nu = [L : F(\alpha)]$. Then we have

$$L = F\big(a\alpha + b\big(\nu\beta - \mathrm{Tr}_{L/F(\alpha)}(\beta)\big)\big).$$

Proof

Let $\varepsilon = a\alpha + b(\nu\beta - \mathrm{Tr}_{L/F(\alpha)}(\beta)) \in L$. Then we have

$$\begin{aligned}\mathrm{Tr}_{L/F(\alpha)}(\varepsilon) &= a\alpha\,\mathrm{Tr}_{L/F(\alpha)}(1) + b\nu\,\mathrm{Tr}_{L/F(\alpha)}(\beta)\\ &\quad - b\,\mathrm{Tr}_{L/F(\alpha)}(\beta)\,\mathrm{Tr}_{L/F(\alpha)}(1)\\ &= a\alpha\nu.\end{aligned} \tag{6.2}$$

Since L is an abelian extension of F, so is $F(\varepsilon)$ by Galois theory. Thus, $\varepsilon^\sigma \in F(\varepsilon)$ for any $\sigma \in \mathrm{Gal}(L/F)$, and hence, $\mathrm{Tr}_{L/F(\alpha)}(\varepsilon) \in F(\varepsilon)$. This implies that $\alpha \in F(\varepsilon)$

by (6.2). Therefore, we obtain

$$F(\varepsilon) = F(\alpha, \varepsilon) = F\big(\alpha, \varepsilon - a\alpha + b\,\mathrm{Tr}_{L/F(\alpha)}(\beta)\big) = F(\alpha, b\nu\beta) = L. \qquad \square$$

THEOREM 6.4

Let ℓ and p be odd primes, let $n = (\ell-1)/2$, and let $\mu \in \mathbb{Z}_{>0}$. Let $\mathbf{r}$, $\mathbf{s}$, z_ℓ, and $A_\ell(\mathbf{r},\mathbf{s})$ be as above. Assume that z_ℓ is neither a zero nor a pole of $\prod_{i=1}^{n+1} \Phi_{[\mathbf{r},\mathbf{s};\mu,i]}(z)_p$. If $p \nmid \ell h_\ell^+ n \cdot \det(A_\ell(\mathbf{r},\mathbf{s}))$, then we have

$$K_{2\mu-1-\alpha} = k_{2\mu-1-\alpha}\Big(\sum_{i=1}^{n+1} \Phi_{[\mathbf{r},\mathbf{s};\mu,i]}(z_\ell)_p^{p^\alpha}\Big) \tag{6.3}$$

for $\alpha = 0, 1, \ldots, \mu-1$. Moreover, if $\dim_{\mathbb{Z}/p\mathbb{Z}}(H_1/S_2) = n-1$, then we have

$$k_{2\mu-\alpha} = k_\mu\Big(\sum_{i=1}^{n+1} \Phi_{[\mathbf{r},\mathbf{s};\mu,i]}(z_\ell)_p^{p^\alpha}\Big) \tag{6.4}$$

for $\alpha = 0, 1, \ldots, \mu-1$.

Proof

Let $\mathbf{x}_{\mu,i} = r_i/p^\mu$ and $\mathbf{y}_{\mu,i} = s_i/p^\mu$ for each μ and i. Then $\mathbf{x}_{\mu,i} = \mathbf{x}_{1,i}/p^{\mu-1}$ and $\mathbf{y}_{\mu,i} = \mathbf{y}_{1,i}/p^{\mu-1}$. By Lemma 6.1, $\Phi_{[\mathbf{r},\mathbf{s};\mu,i]}(z_\ell)_p^{p^\alpha} \in K_{2\mu-1-\alpha}$. It then follows from (6.1) that for $1 \le i, j \le n+1$

$$\begin{aligned}
&\big(\Phi_{[\mathbf{r},\mathbf{s};\mu,i]}(z_\ell)_p^{p^\alpha}\big)^{\left(\frac{K_{2\mu-1-\alpha}/k}{(\omega_{2\mu-1-\alpha,j})}\right)} \\
&\quad = e(-p^{2\mu-1} \cdot {}^t\mathbf{x}_{\mu,i}\mathbf{y}_{\mu,i}) e\Big(\frac{{}^t\mathbf{x}_{\mu,i} b_{2\mu-1,j} - {}^t a_{2\mu-1,j}\mathbf{y}_{\mu,i}}{2}\Big) \Phi_{[\mathbf{r},\mathbf{s};\mu,i]}(z_\ell)_p^{p^\alpha},
\end{aligned}$$

where $a_{2\mu-1,j}, b_{2\mu-1,j} \in 2p^{\mu-1}\mathbb{Z}^n$ such that

$$\begin{aligned}
\begin{bmatrix} a_{2\mu-1,j} \\ b_{2\mu-1,j} \end{bmatrix} &= 2p^{2\mu-1} \cdot {}^t h\big(\varphi^+(\zeta^j)\big) \begin{bmatrix} \mathbf{x}_{\mu,i} \\ \mathbf{y}_{\mu,i} \end{bmatrix} \\
&= 2p^\mu \cdot {}^t h\big(\varphi^+(\zeta^j)\big) \begin{bmatrix} \mathbf{x}_{1,i} \\ \mathbf{y}_{1,i} \end{bmatrix} \\
&= p^{\mu-1} \begin{bmatrix} a_{1,j} \\ b_{1,j} \end{bmatrix}.
\end{aligned}$$

We ensure that

$$\begin{aligned}
&\big(\Phi_{[\mathbf{r},\mathbf{s};\mu,i]}(z_\ell)_p^{p^\alpha}\big)^{\left(\frac{K_{2\mu-1-\alpha}/k}{(\omega_{2\mu-1-\alpha,j})}\right)} \\
&\quad = e(-p \cdot {}^t\mathbf{x}_{1,i}\mathbf{y}_{1,i}) e\Big(\frac{{}^t\mathbf{x}_{1,i} b_{1,j} - {}^t a_{1,j}\mathbf{y}_{1,i}}{2}\Big) \Phi_{[\mathbf{r},\mathbf{s};\mu,i]}(z_\ell)_p^{p^\alpha} \\
&\quad = \zeta_p^{c_{ij}} \Phi_{[\mathbf{r},\mathbf{s};\mu,i]}(z_\ell)_p^{p^\alpha},
\end{aligned} \tag{6.5}$$

where c_{ij} is the (i,j)th entry of $A_\ell(\mathbf{r},\mathbf{s})$. Here, we observe that for $1 \le i \le n+1$ there exists $\gamma_i \in k_{2\mu-1-\alpha}(\Phi_{[\mathbf{r},\mathbf{s};\mu,1]}(z_\ell)_p^{p^\alpha}, \Phi_{[\mathbf{r},\mathbf{s};\mu,2]}(z_\ell)_p^{p^\alpha}, \ldots, \Phi_{[\mathbf{r},\mathbf{s};\mu,n+1]}(z_\ell)_p^{p^\alpha})$

with

$$\gamma_i^{\left(\frac{K_{2\mu-1-\alpha}/k}{(\omega_{2\mu-1-\alpha},j)}\right)}=\begin{cases}\zeta_p\gamma_i & \text{if } j=i,\\ \gamma_i & \text{if } j\neq i,\end{cases}$$

because $p\nmid \det(A_\ell(\mathbf{r},\mathbf{s}))$. Since $|\operatorname{Gal}(K_{2\mu-1-\alpha}/k_{2\mu-1-\alpha})|\le p^{n+1}$ by (4.1), we deduce

(6.6)
$$\begin{aligned}K_{2\mu-1-\alpha}&=k_{2\mu-1-\alpha}(\gamma_1,\gamma_2,\dots,\gamma_{n+1})\\&=k_{2\mu-1-\alpha}\big(\Phi_{[\mathbf{r},\mathbf{s};\mu,1]}(z_\ell)_p^{p^\alpha},\Phi_{[\mathbf{r},\mathbf{s};\mu,2]}(z_\ell)_p^{p^\alpha},\dots,\Phi_{[\mathbf{r},\mathbf{s};\mu,n+1]}(z_\ell)_p^{p^\alpha}\big).\end{aligned}$$

Now, let $L_i=k_{2\mu-1-\alpha}(\Phi_{[\mathbf{r},\mathbf{s};\mu,1]}(z_\ell)_p^{p^\alpha},\Phi_{[\mathbf{r},\mathbf{s};\mu,2]}(z_\ell)_p^{p^\alpha},\dots,\Phi_{[\mathbf{r},\mathbf{s};\mu,i]}(z_\ell)_p^{p^\alpha})$ for each $1\le i\le n+1$. Suppose that $L_m=k_{2\mu-1-\alpha}(\sum_{i=1}^m\Phi_{[\mathbf{r},\mathbf{s};\mu,i]}(z_\ell)_p^{p^\alpha})$ for some integer $1\le m\le n$. Note that $[L_{m+1}:L_m]=p$ and

$$\operatorname{Tr}_{L_{m+1}/L_m}\big(\Phi_{[\mathbf{r},\mathbf{s};\mu,m+1]}(z_\ell)_p^{p^\alpha}\big)=\sum_{j=0}^{p-1}\zeta_p^j\Phi_{[\mathbf{r},\mathbf{s};\mu,m+1]}(z_\ell)_p^{p^\alpha}=0,$$

due to the fact that $\sum_{j=0}^{p-1}\zeta_p^j=0$. Hence, if we take $a=1$ and $b=1/p$, then by Lemma 6.3 we obtain

$$\begin{aligned}L_{m+1}&=k_{2\mu-1-\alpha}\Big(\sum_{i=1}^m\Phi_{[\mathbf{r},\mathbf{s};\mu,i]}(z_\ell)_p^{p^\alpha},\Phi_{[\mathbf{r},\mathbf{s};\mu,m+1]}(z_\ell)_p^{p^\alpha}\Big)\\&=k_{2\mu-1-\alpha}\Big(\sum_{i=1}^{m+1}\Phi_{[\mathbf{r},\mathbf{s};\mu,i]}(z_\ell)_p^{p^\alpha}\Big).\end{aligned}$$

Therefore, (6.3) is proved by induction and (6.6).

If $\dim_{\mathbb{Z}/p\mathbb{Z}}(H_1/S_2)=n-1$, then by the proof of Corollary 4.6 we get

$$\big|\operatorname{Gal}(k_{2\mu-\alpha}/k_{2\mu-1-\alpha})\big|=p^{n+1}.$$

Since $|\operatorname{Gal}(K_{2\mu-1-\alpha}/k_{2\mu-1-\alpha})|=p^{n+1}$ and $K_{2\mu-1-\alpha}\subset k_{2\mu-\alpha}$, we conclude that $K_{2\mu-1-\alpha}=k_{2\mu-\alpha}$. Hence, by (6.6)

$$\begin{aligned}k_{2\mu-\alpha}&=k_{2\mu-1-\alpha}\big(\Phi_{[\mathbf{r},\mathbf{s};\mu,1]}(z_\ell)_p^{p^\alpha},\Phi_{[\mathbf{r},\mathbf{s};\mu,2]}(z_\ell)_p^{p^\alpha},\dots,\Phi_{[\mathbf{r},\mathbf{s};\mu,n+1]}(z_\ell)_p^{p^\alpha}\big)\\&=k_\mu\big(\Phi_{[\mathbf{r},\mathbf{s};\mu,1]}(z_\ell)_p^{p^\alpha},\Phi_{[\mathbf{r},\mathbf{s};\mu,2]}(z_\ell)_p^{p^\alpha},\dots,\Phi_{[\mathbf{r},\mathbf{s};\mu,n+1]}(z_\ell)_p^{p^\alpha}\big)\end{aligned}$$

for $\alpha=0,1,\dots,\mu-1$. Let $L_i'=k_\mu(\Phi_{[\mathbf{r},\mathbf{s};\mu,1]}(z_\ell)_p^{p^\alpha},\Phi_{[\mathbf{r},\mathbf{s};\mu,2]}(z_\ell)_p^{p^\alpha},\dots,\Phi_{[\mathbf{r},\mathbf{s};\mu,i]}(z_\ell)_p^{p^\alpha})$ for each $1\le i\le n+1$. Suppose that $L_m'=k_\mu(\sum_{i=1}^m\Phi_{[\mathbf{r},\mathbf{s};\mu,i]}(z_\ell)_p^{p^\alpha})$ for some integer $1\le m\le n$. Then we have

$$\begin{aligned}\operatorname{Tr}_{L_{m+1}/L_m'}\big(\Phi_{[\mathbf{r},\mathbf{s};\mu,m+1]}(z_\ell)_p^{p^\alpha}\big)&=\operatorname{Tr}_{L_m/L_m'}\big(\operatorname{Tr}_{L_{m+1}/L_m}\big(\Phi_{[\mathbf{r},\mathbf{s};\mu,m+1]}(z_\ell)_p^{p^\alpha}\big)\big)\ (=0)\\&=\operatorname{Tr}_{L_{m+1}'/L_m'}\big(\operatorname{Tr}_{L_{m+1}/L_{m+1}'}\big(\Phi_{[\mathbf{r},\mathbf{s};\mu,m+1]}(z_\ell)_p^{p^\alpha}\big)\big)\\&=[L_{m+1}:L_{m+1}']\cdot\operatorname{Tr}_{L_{m+1}'/L_m'}\big(\Phi_{[\mathbf{r},\mathbf{s};\mu,m+1]}(z_\ell)_p^{p^\alpha}\big),\end{aligned}$$

and so $\mathrm{Tr}_{L'_{m+1}/L'_m}(\Phi_{[\mathbf{r},\mathbf{s};\mu,m+1]}(z_\ell)_p^{p^\alpha}) = 0$. Therefore, by Lemma 6.3

$$L'_{m+1} = k_\mu\Big(\sum_{i=1}^{m}\Phi_{[\mathbf{r},\mathbf{s};\mu,i]}(z_\ell)_p^{p^\alpha}, \Phi_{[\mathbf{r},\mathbf{s};\mu,m+1]}(z_\ell)_p^{p^\alpha}\Big)$$
$$= k_\mu\Big(\sum_{i=1}^{m+1}\Phi_{[\mathbf{r},\mathbf{s};\mu,i]}(z_\ell)_p^{p^\alpha}\Big),$$

and (6.4) is proved again by induction. □

Although we omit in the above theorem the case where p divides $\det(A_\ell(\mathbf{r},\mathbf{s}))$, by utilizing Theorem 4.5 we might find suitable generators of K_μ over k_μ for each $\mu \in \mathbb{Z}_{>0}$.

Let $\mathbf{r}_0 = [r_i]_{1\le i\le n+1}$ and $\mathbf{s}_0 = [s_i]_{1\le i\le n+1}$, where $r_i = {}^t[1\ 0\ \cdots\ 0] \in \mathbb{Z}^n$ and $s_i = {}^t[(s_i)_j]_{1\le j\le n} \in \mathbb{Z}^n$ for $1 \le i \le n+1$ with

$$(s_i)_j = \begin{cases} 1 & \text{if } j < i, \\ 0 & \text{otherwise.} \end{cases}$$

Here we observe that $\Phi_{[\mathbf{r}_0,\mathbf{s}_0;\mu,i]}(z)_p$ is not identically zero for all μ and i by Proposition 5.3.

COROLLARY 6.5

Let ℓ and p be odd primes, and let z_ℓ be as above. Put $n = (\ell-1)/2$, and let $\mu \in \mathbb{Z}_{>0}$. Further, we assume that z_ℓ is not a zero of $\prod_{i=1}^{n+1}\Phi_{[\mathbf{r}_0,\mathbf{s}_0;\mu,i]}(z)_p$.

(i) *Let $\ell = 7$. If $p \ne 3, 7$, then we have*

$$K_{2\mu-1-\alpha} = k_{2\mu-1-\alpha}\Big(\sum_{i=1}^{4}\Phi_{[\mathbf{r}_0,\mathbf{s}_0;\mu,i]}(z_7)_p^{p^\alpha}\Big) \tag{6.7}$$

for $0 \le \alpha \le \mu-1$.

(ii) *Let $\ell = 11$. If $p \ne 3, 5, 11$, then we have*

$$K_{2\mu-1-\alpha} = k_{2\mu-1-\alpha}\Big(\sum_{i=1}^{6}\Phi_{[\mathbf{r}_0,\mathbf{s}_0;\mu,i]}(z_{11})_p^{p^\alpha}\Big) \tag{6.8}$$

for $0 \le \alpha \le \mu-1$. If $p = 3$, then we get

$$K_{2\mu-1-\alpha} = k_{2\mu-1-\alpha}\Big(\sum_{i=1}^{5}\Phi_{[\mathbf{r}_0,\mathbf{s}_0;\mu,i]}(z_{11})_3^{3^\alpha}\Big). \tag{6.9}$$

(iii) *Let $\ell = 13$. If $p \ne 3, 5, 13$, then we have*

$$K_{2\mu-1-\alpha} = k_{2\mu-1-\alpha}\Big(\sum_{i=1}^{7}\Phi_{[\mathbf{r}_0,\mathbf{s}_0;\mu,i]}(z_{13})_p^{p^\alpha}\Big) \tag{6.10}$$

for $0 \le \alpha \le \mu-1$. If $p = 5$, then we obtain

$$K_{2\mu-1-\alpha} = k_{2\mu-1-\alpha}\Big(\sum_{i=1}^{6}\Phi_{[\mathbf{r}_0,\mathbf{s}_0;\mu,i]}(z_{13})_5^{5^\alpha}\Big). \tag{6.11}$$

(iv) *Let* $\ell = 5$. *Then we have*

$$K_{2\mu-1-\alpha} = k_{2\mu-1-\alpha}\big(\zeta_{p^{2\mu-\alpha}} + \Phi_{[\mathbf{r}_0,\mathbf{s}_0;\mu,1]}(z_5)_p^{p^\alpha} + \Phi_{[\mathbf{r}_0,\mathbf{s}_0;\mu,3]}(z_5)_p^{p^\alpha}\big) \tag{6.12}$$

for $0 \le \alpha \le \mu - 1$.

Proof

Let the matrix $M_\ell(p)$ be as in Lemma 4.4. Note that $h_\ell^+ = 1$ for $\ell \le 67$ (see [30, p. 352]). We can show that z_ℓ is not a pole of $\prod_{i=1}^{n+1} \Phi_{[\mathbf{r}_0,\mathbf{s}_0;\mu,i]}(z)_p$ for $\ell \le 17$ by utilizing the `RiemannTheta` command in Maple.

(i) Using (6.1) we can find $\Phi_{[\mathbf{r}_0,\mathbf{s}_0;1,i]}(z_7)_p^{\left(\frac{K_1/k}{(\omega_{1,j})}\right)}$ for each $1 \le i, j \le 4$ as follows:

$$\begin{matrix} \\ \Phi_{[\mathbf{r}_0,\mathbf{s}_0;1,1]}(z_7)_p \\ \Phi_{[\mathbf{r}_0,\mathbf{s}_0;1,2]}(z_7)_p \\ \Phi_{[\mathbf{r}_0,\mathbf{s}_0;1,3]}(z_7)_p \\ \Phi_{[\mathbf{r}_0,\mathbf{s}_0;1,4]}(z_7)_p \end{matrix} \begin{bmatrix} \left(\frac{K_1/k}{(\omega_{1,1})}\right) & \left(\frac{K_1/k}{(\omega_{1,2})}\right) & \left(\frac{K_1/k}{(\omega_{1,3})}\right) & \left(\frac{K_1/k}{(\omega_{1,4})}\right) \\ -1 & -1 & -1 & 1 \\ -2 & -4 & -2 & 0 \\ 0 & -10 & -4 & 2 \\ -3 & -13 & -11 & 9 \end{bmatrix} = A_7(\mathbf{r}_0, \mathbf{s}_0).$$

Since $\det(A_7(\mathbf{r}_0, \mathbf{s}_0)) = 2^6$ is prime to p, (6.7) is true by Theorem 6.4.

(ii) First, suppose that $p \ne 3, 5, 11$. In a similar way as in (i) we obtain

$$A_{11}(\mathbf{r}_0, \mathbf{s}_0) = \begin{bmatrix} -1 & -1 & -1 & -1 & -1 & 1 \\ -2 & -4 & -2 & -4 & -2 & 0 \\ -4 & -6 & -4 & -10 & 0 & -2 \\ -7 & -3 & -11 & -21 & -3 & 1 \\ -7 & -5 & -25 & -29 & -1 & -1 \\ -10 & -2 & -48 & -34 & -6 & 4 \end{bmatrix}.$$

Since $\det(A_{11}(\mathbf{r}_0, \mathbf{s}_0)) = 2^7 \cdot 3 \cdot 5^2$ is prime to p, we get (6.8) by Theorem 6.4. If $p = 3$, then the rank of $M_{11}(3)$ is equal to 5. Since $p \nmid 11 \cdot 5$, by Theorem 4.5 we deduce $\mathrm{Gal}(K_\mu/k_\mu) \cong (\mathbb{Z}/3\mathbb{Z})^5$ for all $\mu \in \mathbb{Z}_{>0}$. We observe that the determinant of the matrix

$$\begin{matrix} \\ \Phi_{[\mathbf{r}_0,\mathbf{s}_0;1,1]}(z_{11})_3 \\ \Phi_{[\mathbf{r}_0,\mathbf{s}_0;1,2]}(z_{11})_3 \\ \Phi_{[\mathbf{r}_0,\mathbf{s}_0;1,3]}(z_{11})_3 \\ \Phi_{[\mathbf{r}_0,\mathbf{s}_0;1,4]}(z_{11})_3 \\ \Phi_{[\mathbf{r}_0,\mathbf{s}_0;1,5]}(z_{11})_3 \end{matrix} \begin{bmatrix} \left(\frac{K_1/k}{(\omega_{1,2})}\right) & \left(\frac{K_1/k}{(\omega_{1,3})}\right) & \left(\frac{K_1/k}{(\omega_{1,4})}\right) & \left(\frac{K_1/k}{(\omega_{1,5})}\right) & \left(\frac{K_1/k}{(\omega_{1,6})}\right) \\ -1 & -1 & -1 & -1 & 1 \\ -4 & -2 & -4 & -2 & 0 \\ -6 & -4 & -10 & 0 & -2 \\ -3 & -11 & -21 & -3 & 1 \\ -5 & -25 & -29 & -1 & -1 \end{bmatrix}$$

is equal to $2^5 \cdot 5 \cdot 11$, which is prime to 3. Using Lemma 6.3 and (6.5) we can conclude (6.9).

(iii) First, suppose that $p \neq 3, 5, 13$. Then we derive

$$A_{13}(\mathbf{r}_0, \mathbf{s}_0) = \begin{bmatrix} -1 & -1 & -1 & -1 & -1 & -1 & 1 \\ -2 & -4 & -2 & -4 & -2 & -4 & 2 \\ 0 & -10 & -4 & -6 & -4 & -10 & 8 \\ 5 & -19 & -7 & -11 & -11 & -13 & 11 \\ 7 & -35 & -13 & -13 & -19 & -15 & 13 \\ 2 & -60 & -18 & -8 & -32 & -22 & 20 \\ -10 & -84 & -28 & 2 & -54 & -22 & 20 \end{bmatrix}.$$

Since $\det(A_{13}(\mathbf{r}_0, \mathbf{s}_0)) = -2^{12} \cdot 5^2$ is prime to p, we have (6.10) again by Theorem 6.4. If $p = 5$, then the rank of $M_{13}(5)$ is equal to 6. Since $p \nmid 13 \cdot 6$, it follows from Theorem 4.5 that $\mathrm{Gal}(K_\mu/k_\mu) \cong (\mathbb{Z}/5\mathbb{Z})^6$ for all $\mu \in \mathbb{Z}_{>0}$. Observe that the determinant of the matrix

$$\begin{array}{c} \\ \Phi_{[\mathbf{r}_0,\mathbf{s}_0;1,1]}(z_{13})_5 \\ \Phi_{[\mathbf{r}_0,\mathbf{s}_0;1,2]}(z_{13})_5 \\ \Phi_{[\mathbf{r}_0,\mathbf{s}_0;1,3]}(z_{13})_5 \\ \Phi_{[\mathbf{r}_0,\mathbf{s}_0;1,4]}(z_{13})_5 \\ \Phi_{[\mathbf{r}_0,\mathbf{s}_0;1,5]}(z_{13})_5 \\ \Phi_{[\mathbf{r}_0,\mathbf{s}_0;1,6]}(z_{13})_5 \end{array} \begin{array}{c} \begin{matrix} \left(\frac{K_1/k}{(\omega_{1,2})}\right) & \left(\frac{K_1/k}{(\omega_{1,3})}\right) & \left(\frac{K_1/k}{(\omega_{1,4})}\right) & \left(\frac{K_1/k}{(\omega_{1,5})}\right) & \left(\frac{K_1/k}{(\omega_{1,6})}\right) & \left(\frac{K_1/k}{(\omega_{1,7})}\right) \end{matrix} \\ \begin{bmatrix} -1 & -1 & -1 & -1 & -1 & 1 \\ -4 & -2 & -4 & -2 & -4 & 2 \\ -10 & -4 & -6 & -4 & -10 & 8 \\ -19 & -7 & -11 & -11 & -13 & 11 \\ -35 & -13 & -13 & -19 & -15 & 13 \\ -60 & -18 & -8 & -32 & -22 & 20 \end{bmatrix} \end{array}$$

is equal to $-2^7 \cdot 31$, which is prime to 5. Using Lemma 6.3 and (6.5) we can deduce (6.11).

(iv) In this case, $\det(A_5(\mathbf{r}_0, \mathbf{s}_0)) = 0$ so we should find another generator of $K_{2\mu-1-\alpha}$ over $k_{2\mu-1-\alpha}$. By [14, p. 316], $H_{2\mu-1-\alpha}/S_{2\mu-\alpha}$ is generated by real units of k for any odd prime p. Using the idea in the proof of Theorem 4.5, one can show that $(\varphi^*(S_{2\mu-1-\alpha}) \cap H_{2\mu-1-\alpha})/S_{2\mu-\alpha} = \{0\}$, and so $\Phi_{[\mathbf{r}_0,\mathbf{s}_0;\mu,i]}(z_5)_p^{p^\alpha} \in K_{2\mu-1-\alpha}$ for $1 \leq i \leq 3$. Note that $\zeta_{p^{2\mu-\alpha}} \in \mathcal{F}_{2p^{2\mu-\alpha}}$ is $R_{2p^{2\mu-\alpha}}$-invariant; hence, $\zeta_{p^{2\mu-\alpha}} \in K_{2\mu-1-\alpha}$ by Proposition 3.2. Since $N_{k/\mathbb{Q}}(\omega_{2\mu-1-\alpha,j}) \equiv 1 - 2p^{2\mu-1-\alpha} \pmod{2p^{2\mu-\alpha}}$ for $1 \leq j \leq 3$, we get

$$\zeta_{p^{2\mu-\alpha}}^{\left(\frac{K_{2\mu-1-\alpha}/k}{(\omega_{2\mu-1-\alpha,j})}\right)} = \zeta_p^{-2}\zeta_{p^{2\mu-\alpha}} \quad \text{for } 1 \leq j \leq 3. \tag{6.13}$$

Now, observe that the determinant of the matrix

$$\begin{array}{c} \\ \zeta_{p^2} \\ \Phi_{[\mathbf{r}_0,\mathbf{s}_0;1,1]}(z_5)_p \\ \Phi_{[\mathbf{r}_0,\mathbf{s}_0;1,3]}(z_5)_p \end{array} \begin{array}{c} \begin{matrix} \left(\frac{K_1/k}{(\omega_{1,1})}\right) & \left(\frac{K_1/k}{(\omega_{1,2})}\right) & \left(\frac{K_1/k}{(\omega_{1,3})}\right) \end{matrix} \\ \begin{bmatrix} -2 & -2 & -2 \\ -1 & -1 & 1 \\ -4 & -6 & 4 \end{bmatrix} \end{array}$$

is equal to -2^3, which is prime to p. Therefore, we obtain (6.12) by Lemma 6.3, (6.5), and (6.13). □

REMARK 6.6

(i) Especially when $\mu = 1$, Corollary 6.5(iv) is reduced to Komatsu's work (see [14, Proposition 1]) with a few different ingredients.

Table 2

ℓ	prime factors of $\det(A_\ell(\mathbf{r}_0, \mathbf{s}_0))$
3	2
5	0
7	2
11	2, 3, 5
13	2, 5
17	2, 7, 17, 43
19	2, 3, 36137
23	2, 3, 11, 13, 29, 89, 241
29	2, 3, 5, 13, 113, 58057291
31	2, 3, 31, 109621, 1216387
37	2, 5, 13, 37, 53, 109, 10138325056259
41	2, 5, 11, 17, 41, 439, 1667, 166013, 203381
43	2, 3, 19, 43, 211, 281345721890371109
47	2, 5, 83, 139, 5323, 178481, 6167669171116393
53	2, 3, 5, 139, 157, 1613, 4889, 1579367, 28153859844430949
59	2, 3, 59, 233, 3033169, 189946818040963445273025207051 7
61	2, 5, 11, 13, 41, 1321, 1861, 1142941857599125232990619467569
67	2, 3, 67, 683, 12739, 20857, 513881, 1858283767, 986862333655510350967
71	2, 5, 7, 31, 79, 127, 1129, 79241, 122921, 68755411, 1190061671, 3087543529906501
73	2, 7, 73, 79, 89, 16747, 134353, 5754557119657, 1150806776867233, 1190899
79	2, 5, 7, 13, 29, 53, 1427, 3847, 8191, 121369, 377911, 1842497, 51176893, 357204083, 32170088152177
83	2, 3, 13, 17387, 279405653, 430592619820725846267877053013 51, 8831418697, 758583423553
89	2, 17, 23, 89, 113, 313629821584641896139082338756559409, 4504769, 118401449, 22482210593

(ii) Table 2 gives the prime factors of $\det(A_\ell(\mathbf{r}_0, \mathbf{s}_0))$ for $\ell \leq 89$.

References

[1] T. M. Apostol, *Introduction to Analytic Number Theory*, Undergrad. Texts Math., Springer, New York, 1976. MR 0434929.

[2] B. Cais and B. Conrad, *Modular curves and Ramanujan's continued fraction*, J. Reine Angew. Math. **597** (2006), 27–104. MR 2264315. DOI 10.1515/CRELLE.2006.063.

[3] I. Chen and N. Yui, "Singular values of Thompson series" in *Groups, Difference Sets, and the Monster (Columbus, OH, 1993)*, Ohio State Univ. Math. Res. Inst. Publ. **4**, de Gruyter, Berlin, 1996, 255–326. MR 1400423.

[4] B. Cho and J. K. Koo, *Construction of class fields over imaginary quadratic fields and applications*, Q. J. Math. **61** (2010), 199–216. MR 2646085. DOI 10.1093/qmath/han035.

[5] J. Cougnard, *Conditions nécessaires de monogénéité: Application aux extensions cycliques de degré premier $\ell \geq 5$ d'un corps quadratique imaginaire*, J. Lond. Math. Soc. (2) **37** (1988), 73–87. MR 0921746. DOI 10.1112/jlms/s2-37.121.73.

[6] J. Cougnard and M. Vérant, *Monogénéité de l'anneau des entiers de corps de classes de rayon de corps quadratiques*, Sém. Théor. Nombres Bordeaux (2) **4** (1992), 53–74. MR 1183918.

[7] D. A. Cox, *Primes of the Form $x^2 + ny^2$: Fermat, Class Field Theory and Complex Multiplication*, Wiley, New York, 1989. MR 1028322.

[8] D. A. Cox, J. McKay, and P. Stevenhagen, *Principal moduli and class fields*, Bull. Lond. Math. Soc. **36** (2004), 3–12. MR 2011972. DOI 10.1112/S0024609303002583.

[9] M. Eichler, *Der Hilbertsche Klassenkörper eines imaginärquadratischen Zahlkörpers*, Math. Z. **64** (1956), 229–242. MR 0086096.

[10] H. Hasse, *Neue Bergründung der komplexen Multiplikation, I: Einordnung in die allgemeine Klassenkörpertheorie*, J. Reine Angew. Math. **157** (1927), 115–140; *II: Aufbau ohne Benutzung der allgemeinen Klassenkörpertheorie*, **165** (1931), 64–88. MR 1581113; MR 1581274. DOI 10.1515/crll.1931.165.64.

[11] J. Igusa, *On the graded ring of theta-constants, II*, Amer. J. Math. **88** (1966), 221–236. MR 0200482.

[12] H. Y. Jung, J. K. Koo, and D. H. Shin, *Normal bases of ray class fields over imaginary quadratic fields*, Math. Z. **271** (2012), 109–116. MR 2917135. DOI 10.1007/s00209-011-0854-2.

[13] H. Klingen, *Introductory Lectures on Siegel Modular Forms*, Cambridge Stud. Adv. Math. **20**, Cambridge Univ. Press, Cambridge, 1990. MR 1046630. DOI 10.1017/CBO9780511619878.

[14] K. Komatsu, *Construction of a normal basis by special values of Siegel modular functions*, Proc. Amer. Math. Soc. **128** (2000), 315–323. MR 1707153. DOI 10.1090/S0002-9939-99-05601-4.

[15] S. Lang, *Elliptic Functions*, with an appendix by J. Tate, 2nd ed., Grad. Texts in Math. **112**, Springer, New York, 1987. MR 0890960. DOI 10.1007/978-1-4612-4752-4.

[16] J. J. Liang, *On the integral basis of the maximal real subfield of a cyclotomic field*, J. Reine Angew. Math. **286/287** (1976), 223–226. MR 0419402.

[17] B. Mazur, *How can we construct abelian Galois extensions of basic number fields?*, Bull. Amer. Math. Soc. (N.S.) **48** (2011), 155–209. MR 2774089. DOI 10.1090/S0273-0979-2011-01326-X.

[18] K. Ramachandra, *Some applications of Kronecker's limit formulas*, Ann. of Math. (2) **80** (1964), 104–148. MR 0164950.

[19] K. A. Ribet, *A modular construction of unramified p-extensions of* $\mathbb{Q}(\mu_p)$, Invent. Math. **34** (1976), 151–162. MR 0419403.

[20] R. Schertz, *L-Reihen in imaginär-quadratischen Zahlkörpern und ihre Anwendung auf Klassenzahlprobleme bei quadratischen und biquadratischen Zahlkörpern, I*, J. Reine Angew. Math. **262/263** (1973), 120–133. MR 0332731.

[21] ———, *Weber's class invariants revisited*, J. Théor. Nombres Bordeaux **14** (2002), 325–343. MR 1926005.

[22] ———, *Complex Multiplication*, New Math. Monogr. **15**, Cambridge Univ. Press, Cambridge, 2010. MR 2641876. DOI 10.1017/CBO9780511776892.

[23] G. Shimura, *On the class-fields obtained by complex multiplication of abelian varieties*, Osaka J. Math. **14** (1962), 33–44. MR 0170893.

[24] ———, *On canonical models of arithmetic quotients of bounded symmetric domains*, Ann. of Math. (2) **91** (1970), 144–222. MR 0257031.

[25] ———, *On canonical models of arithmetic quotients of bounded symmetric domains, II*, Ann. of Math. (2) **92** (1970), 528–549. MR 0292758.

[26] ———, *Theta functions with complex multiplication*, Duke Math. J. **43** (1976), 673–696. MR 0424705.

[27] ———, *Abelian Varieties with Complex Multiplication and Modular Functions*, Princeton Math. Ser. **46**, Princeton Univ. Press, Princeton, 1998. MR 1492449.

[28] P. Stevenhagen, "Hilbert's 12th problem, complex multiplication and Shimura reciprocity" in *Class Field Theory—Its Centenary and Prospect (Tokyo, 1998)*, Adv. Stud. Pure Math. **30**, Math. Soc. Japan, Tokyo, 2001, 161–176. MR 1846457.

[29] T. Takagi, *Über eine Theorie des relativ-Abelschen Zahlkörpers*, J. Coll. Sci. Univ. Tokyo **41** (1920), 1–133.

[30] L. C. Washington, *Introduction to Cyclotomic Fields*, Grad. Texts in Math. **83**, Springer, New York, 1982. MR 0718674. DOI 10.1007/978-1-4684-0133-2.

Koo: Department of Mathematical Sciences, KAIST, Daejeon, Republic of Korea; jkkoo@math.kaist.ac.kr

Yoon: Department of Mathematical Sciences, KAIST, Daejeon, Republic of Korea; math_dsyoon@kaist.ac.kr