Rev. Mat. Iberoam. **30** (2014), no. 4, 1489–1498
DOI 10.4171/RMI/823

Application of Weierstrass units to relative power integral bases

Ho Yun Jung, Ja Kyung Koo and Dong Hwa Shin

Abstract. Let K be an imaginary quadratic field not equal to $\mathbb{Q}(\sqrt{-1})$ or $\mathbb{Q}(\sqrt{-3})$. We construct relative power integral bases between certain abelian extensions of K in terms of Weierstrass units.

1. Introduction

Let L/F be an extension of number fields and let $\mathcal{O}_L$ and $\mathcal{O}_F$ be the rings of integers of L and F, respectively. We say that an element α of L forms a *relative power integral basis* for L/F if $\mathcal{O}_L = \mathcal{O}_F[\alpha]$. For example, if N is a positive integer, then $\zeta_N = e^{2\pi i/N}$ forms a (relative) power integral basis for the extension $\mathbb{Q}(\zeta_N)/\mathbb{Q}$ (see Theorem 2.6 in [21]). In general not much is known about relative power integral bases except for extensions of degree less than or equal to 9 (see references [1]–[12]).

Let K be an imaginary quadratic field not equal to $\mathbb{Q}(\sqrt{-1})$ or $\mathbb{Q}(\sqrt{-3})$. Let m and n be positive integers such that m has at least two prime factors and each prime factor of mn splits in $K/\mathbb{Q}$. In this paper we shall show that a certain Weierstrass unit forms a relative power integral basis for the ray class field modulo (mn) over the compositum of the ray class field modulo (m) and the ring class field of the order of conductor mn of K (Theorem 4.1). To this end, we shall make use of an explicit description of the Shimura reciprocity law in [20] due to Stevenhagen.

2. Weierstrass units

For a positive integer N, let $\Gamma(N)$ be the principal congruence subgroup of level N, namely

$$\Gamma(N) = \{\gamma \in \mathrm{SL}_2(\mathbb{Z}) \mid \gamma \equiv I_2 \pmod{N}\}.$$

Then $\overline{\Gamma}(N) = \langle \Gamma(N), -I_2\rangle/\{\pm I_2\}$ acts on the complex upper half-plane $\mathbb{H}$ by fractional linear transformations.

Mathematics Subject Classification (2010): Primary 11G16; Secondary 11G15, 11Y40.
Keywords: power integral bases, Shimura reciprocity law, Weierstrass units.

Let $\mathcal{F}_N$ be the field of meromorphic modular functions for $\overline{\Gamma}(N)$ (or, of level N) whose Fourier coefficients lie in the Nth cyclotomic field $\mathbb{Q}(\zeta_N)$. As is well known, $\mathcal{F}_1$ is generated by the elliptic modular function

$$j(\tau) = q^{-1} + 744 + 196884q + 21493760q^2 + 864299970q^3 + \cdots \quad (q = e^{2\pi i\tau})$$

over $\mathbb{Q}$ (see Section 6.1 in [18]). 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 Section 6.2 in [18]). Let $\mathcal{R}_N$ and $\mathbb{Q}\mathcal{R}_N$ be the integral closures of $\mathbb{Z}[j(\tau)]$ and $\mathbb{Q}[j(\tau)]$ in $\mathcal{F}_N$, respectively. We call the elements of $(\mathbb{Q}\mathcal{R}_N)^*$ *modular units* of level N. These are precisely those elements of $\mathcal{F}_N$ having neither zeros nor poles on $\mathbb{H}$ (see p. 36 in [15]). In particular, we call the elements of $\mathcal{R}_N^*$ *modular units over* $\mathbb{Z}$ of level N.

Let $\Lambda = [\omega_1, \omega_2]$ $(= \omega_1\mathbb{Z} + \omega_2\mathbb{Z})$ be a lattice in $\mathbb{C}$. The *Weierstrass* $\wp$*-function* relative to Λ is defined by

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

It is a meromorphic function on z, periodic with respect to Λ.

Lemma 2.1. *Let $z_1, z_2 \in \mathbb{C}-\Lambda$. Then, $\wp(z_1;\Lambda) = \wp(z_2;\Lambda)$ if and only if $z_1 \equiv \pm z_2 \pmod{\Lambda}$.*

Proof. See Section 3 of Chapter IV in [19]. □

Let $\left[\begin{smallmatrix} r \\ s \end{smallmatrix}\right] \in (1/N)\mathbb{Z}^2 - \mathbb{Z}^2$ for an integer $N \geq 2$. We define

$$\wp_{\left[\begin{smallmatrix} r \\ s \end{smallmatrix}\right]}(\tau) = \wp(r\tau + s; [\tau, 1]) \quad (\tau \in \mathbb{H}).$$

This is a weakly holomorphic (that is, holomorphic on $\mathbb{H}$) modular form of level N and weight 2 (see Chapter 6 in [16]). We further define

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

which are modular forms of level 1 and weights 4, 6, and 12, respectively. Now we define the *Fricke function* $f_{\left[\begin{smallmatrix} r \\ s \end{smallmatrix}\right]}(\tau)$ by

$$f_{\left[\begin{smallmatrix} r \\ s \end{smallmatrix}\right]}(\tau) = \frac{g_2(\tau)\, g_3(\tau)}{\Delta(\tau)} \wp_{\left[\begin{smallmatrix} r \\ s \end{smallmatrix}\right]}(\tau). \tag{2.1}$$

It depends only on $\pm\left[\begin{smallmatrix} r \\ s \end{smallmatrix}\right] \pmod{\mathbb{Z}^2}$ (see p. 8 in [16]) and is weakly holomorphic because $\Delta(\tau)$ does not vanish on $\mathbb{H}$.

Lemma 2.2. *$f_{\left[\begin{smallmatrix} r \\ s \end{smallmatrix}\right]}(\tau)$ belongs to $\mathcal{F}_N$ and satisfies the transformation formula*

$$f_{\left[\begin{smallmatrix} r \\ s \end{smallmatrix}\right]}(\tau)^\gamma = f_{{}^t\gamma\left[\begin{smallmatrix} r \\ s \end{smallmatrix}\right]}(\tau) \quad (\gamma \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I_2\} \simeq \mathrm{Gal}(\mathcal{F}_N/\mathcal{F}_1)),$$

where ${}^t\gamma$ stands for the transpose of γ.

Proof. See Sections 2 and 3 of Chapter 6 in [16]. □

On the other hand, we define the *Siegel function* $g_{\left[\begin{smallmatrix} r \\ s \end{smallmatrix}\right]}(\tau)$ by

$$g_{\left[\begin{smallmatrix} r \\ s \end{smallmatrix}\right]}(\tau) = -q^{(1/2)(r^2-r+1/6)}e^{\pi is(r-1)}(1-q^r e^{2\pi is}) \prod_{n=1}^{\infty}(1-q^{n+r}e^{2\pi is})(1-q^{n-r}e^{-2\pi is}).$$

Lemma 2.3. *Let M be the primitive denominator of $\left[\begin{smallmatrix} r \\ s \end{smallmatrix}\right]$ (that is, M is the least positive integer so that $Mr, Ms \in \mathbb{Z}$).*

(i) $g_{\left[\begin{smallmatrix} r \\ s \end{smallmatrix}\right]}(\tau)^{12M}$ *and* $g_{\left[\begin{smallmatrix} r \\ s \end{smallmatrix}\right]}(\tau)$ *are modular units of levels M and $12M^2$, respectively.*

(ii) $g_{\left[\begin{smallmatrix} r \\ s \end{smallmatrix}\right]}(\tau)^{12M}$ *depends only on $\pm\left[\begin{smallmatrix} r \\ s \end{smallmatrix}\right] \pmod{\mathbb{Z}^2}$ and satisfies the transformation formula*

$$(g_{\left[\begin{smallmatrix} r \\ s \end{smallmatrix}\right]}(\tau)^{12M})^{\gamma} = g_{{}^t\gamma\left[\begin{smallmatrix} r \\ s \end{smallmatrix}\right]}(\tau)^{12M} \quad (\gamma \in \mathrm{GL}_2(\mathbb{Z}/M\mathbb{Z})/\{\pm I_2\} \simeq \mathrm{Gal}(\mathcal{F}_M/\mathcal{F}_1)).$$

(iii) *Moreover, if M has at least two prime factors, then $g_{\left[\begin{smallmatrix} r \\ s \end{smallmatrix}\right]}(\tau)$ is a modular unit over $\mathbb{Z}$.*

Proof. (i) See Theorem 1.2 in Chapter 2 and Theorems 5.2 and 5.3 in Chapter 3 of [15].

(ii) See Proposition 1.4 in Chapter 2 of [15].

(iii) See Theorem 2.2 (i) in Chapter 2 of [15]. □

Lemma 2.4. *Let $\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right], \left[\begin{smallmatrix} c \\ d \end{smallmatrix}\right] \in \mathbb{Q}^2 - \mathbb{Z}^2$ be such that $\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right] \not\equiv \pm\left[\begin{smallmatrix} c \\ d \end{smallmatrix}\right] \pmod{\mathbb{Z}^2}$. We have the relation*

$$\wp_{\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right]}(\tau) - \wp_{\left[\begin{smallmatrix} c \\ d \end{smallmatrix}\right]}(\tau) = -\frac{g_{\left[\begin{smallmatrix} a+c \\ b+d \end{smallmatrix}\right]}(\tau)g_{\left[\begin{smallmatrix} a-c \\ b-d \end{smallmatrix}\right]}(\tau)\eta(\tau)^4}{g_{\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right]}(\tau)^2 g_{\left[\begin{smallmatrix} c \\ d \end{smallmatrix}\right]}(\tau)^2},$$

where

$$\eta(\tau) = \sqrt{2\pi}\zeta_8 q^{1/24}\prod_{n=1}^{\infty}(1-q^n).$$

Proof. See page 51 of [15]. □

Proposition 2.5. *Consider integers $m \geq 2$ and $n > 0$. The function*

$$h_{m,n}(\tau) = \frac{\wp_{\left[\begin{smallmatrix} 0 \\ 1/mn \end{smallmatrix}\right]}(\tau) - \wp_{\left[\begin{smallmatrix} 1/m \\ 0 \end{smallmatrix}\right]}(\tau)}{\wp_{\left[\begin{smallmatrix} 0 \\ 1/m \end{smallmatrix}\right]}(\tau) - \wp_{\left[\begin{smallmatrix} 1/m \\ 0 \end{smallmatrix}\right]}(\tau)} \tag{2.2}$$

is a modular unit of level mn. If m has at least two prime factors, then $h_{m,n}(\tau)$ is a modular unit over $\mathbb{Z}$.

Proof. It follows from Lemma 2.1 that the denominator of $h_{m,n}(\tau)$ is not the zero function. Furthermore, since

$$h_{m,n}(\tau) = \frac{f_{\left[\begin{smallmatrix} 0 \\ 1/mn \end{smallmatrix}\right]}(\tau) - f_{\left[\begin{smallmatrix} 1/m \\ 0 \end{smallmatrix}\right]}(\tau)}{f_{\left[\begin{smallmatrix} 0 \\ 1/m \end{smallmatrix}\right]}(\tau) - f_{\left[\begin{smallmatrix} 1/m \\ 0 \end{smallmatrix}\right]}(\tau)} \tag{2.3}$$

by Definition (2.1), it belongs to $\mathcal{F}_{mn}$, by Lemma 2.2.

On the other hand, we see that

$$h_{m,n}(\tau) = \frac{-g_{\left[\begin{smallmatrix}1/m\\1/mn\end{smallmatrix}\right]}(\tau)g_{\left[\begin{smallmatrix}-1/m\\1/mn\end{smallmatrix}\right]}(\tau)\eta(\tau)^4/g_{\left[\begin{smallmatrix}0\\1/mn\end{smallmatrix}\right]}(\tau)^2 g_{\left[\begin{smallmatrix}1/m\\0\end{smallmatrix}\right]}(\tau)^2}{-g_{\left[\begin{smallmatrix}1/m\\1/m\end{smallmatrix}\right]}(\tau)g_{\left[\begin{smallmatrix}-1/m\\1/m\end{smallmatrix}\right]}(\tau)\eta(\tau)^4/g_{\left[\begin{smallmatrix}0\\1/m\end{smallmatrix}\right]}(\tau)^2 g_{\left[\begin{smallmatrix}1/m\\0\end{smallmatrix}\right]}(\tau)^2}$$

$$= \frac{g_{\left[\begin{smallmatrix}1/m\\1/mn\end{smallmatrix}\right]}(\tau)g_{\left[\begin{smallmatrix}-1/m\\1/mn\end{smallmatrix}\right]}(\tau)g_{\left[\begin{smallmatrix}0\\1/m\end{smallmatrix}\right]}(\tau)^2}{g_{\left[\begin{smallmatrix}1/m\\1/m\end{smallmatrix}\right]}(\tau)g_{\left[\begin{smallmatrix}-1/m\\1/m\end{smallmatrix}\right]}(\tau)g_{\left[\begin{smallmatrix}0\\1/mn\end{smallmatrix}\right]}(\tau)^2}$$

by Lemma 2.4. This yields, by Lemma 2.3 (i), that $h_{m,n}(\tau)$ is a modular unit. Moreover, if m has at least two prime factors, then each of

$$\begin{bmatrix}1/m\\1/mn\end{bmatrix}, \begin{bmatrix}-1/m\\1/mn\end{bmatrix}, \begin{bmatrix}0\\1/m\end{bmatrix}, \begin{bmatrix}1/m\\1/m\end{bmatrix}, \begin{bmatrix}-1/m\\1/m\end{bmatrix}, \begin{bmatrix}0\\1/mn\end{bmatrix}$$

has primitive denominator with at least two prime factors. Therefore $h_{m,n}(\tau)$ is a modular unit over $\mathbb{Z}$, by Lemma 2.3 (iii). □

Remark 2.6. The modular unit $h_{m,n}(\tau)$ is called a *Weierstrass unit* (see Section 6 in Chapter 2 of [15]).

3. The Shimura reciprocity law

Throughout this section let K be an imaginary quadratic field of discriminant d_K not equal to $\mathbb{Q}(\sqrt{-1})$ or $\mathbb{Q}(\sqrt{-3})$, and set

$$\theta_K = \frac{d_K + \sqrt{d_K}}{2}. \tag{3.1}$$

This belongs to $\mathbb{H}$ and forms a (relative) power integral basis for $K/\mathbb{Q}$. Furthermore, $g_2(\theta_K)$ and $g_3(\theta_K)$ are nonzero (see p. 37 in [16]).

For a nonzero ideal $\mathfrak{f}$ of $\mathcal{O}_K$ we denote the ray class field modulo $\mathfrak{f}$ by $K_{\mathfrak{f}}$. Furthermore, if $\mathcal{O} = [N\theta_K, 1]$ is the order of conductor $N \geq 1$ of K, then we mean the ring class field of the order $\mathcal{O}$ by $H_{\mathcal{O}}$. As a consequence of the main theorem of complex multiplication we have the following lemma.

Lemma 3.1. *Let N be a positive integer.*

(i) *We have $K_{(N)} = K(f(\theta_K) \mid f \in \mathcal{F}_N$ is finite at $\theta_K)$.*

(ii) *If $N \geq 2$, then $K_{(N)} = K_{(1)}(f_{\left[\begin{smallmatrix}0\\1/N\end{smallmatrix}\right]}(\theta_K))$.*

Proof. (i) See the corollary to Theorem 2 in Chapter 10 of [16].

(ii) See the corollary to Theorem 7 in Chapter 10 of [16]. □

Lemma 3.2. *If $\theta \in \mathbb{H}$ is imaginary quadratic, then $j(\theta)$ is an algebraic integer.*

Proof. See Theorem 4.14 in [18]. $\square$

Proposition 3.3. *Consider integers $m \geq 2$ and $n > 0$. Then $h_{m,n}(\theta_K)$ generates $K_{(mn)}$ over $K_{(m)}$. Moreover, if m has at least two prime factors, then $h_{m,n}(\theta_K)$ is a unit of $\mathcal{O}_{K_{(mn)}}$.*

Proof. We first derive that

$$\begin{aligned}
K_{(mn)} &= K_{(1)}(f_{\left[\begin{smallmatrix}0\\1/mn\end{smallmatrix}\right]}(\theta_K)) && \text{(by Lemma 3.1 (ii))}\\
&= K_{(m)}\left(\frac{f_{\left[\begin{smallmatrix}0\\1/mn\end{smallmatrix}\right]}(\theta_K) - f_{\left[\begin{smallmatrix}1/m\\0\end{smallmatrix}\right]}(\theta_K)}{f_{\left[\begin{smallmatrix}0\\1/m\end{smallmatrix}\right]}(\theta_K) - f_{\left[\begin{smallmatrix}1/m\\0\end{smallmatrix}\right]}(\theta_K)}\right) && \text{(by Lemma 3.1 (i))}\\
&= K_{(m)}(h_{m,n}(\theta_K)) && \text{(by (2.3)).}
\end{aligned}$$

If m has at least two prime factors, then $h_{m,n}(\tau)$ is a modular unit over $\mathbb{Z}$ by Proposition 2.5; hence $h_{m,n}(\tau)$ and $h_{m,n}(\tau)^{-1}$ are both integral over $\mathbb{Z}[j(\tau)]$. Therefore we conclude by Lemma 3.2 that $h_{m,n}(\theta_K)$ is a unit as an algebraic integer. $\square$

Lemma 3.4 (Shimura reciprocity law). *Let N be a positive integer and let $\mathcal{O}$ be the order of conductor N of K. Consider the matrix group*

$$W_{K,N} = \left\{ \begin{bmatrix} t - B_K s & -C_K s \\ s & t \end{bmatrix} \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) \mid t, s \in \mathbb{Z}/N\mathbb{Z} \right\},$$

where

$$\min(\theta_K, \mathbb{Q}) = X^2 + B_K X + C_K = X^2 - d_K X + \frac{d_K^2 - d_K}{4}.$$

(i) *The map*

$$\begin{aligned}
W_{K,N}/\{\pm I_2\} &\longrightarrow \mathrm{Gal}(K_{(N)}/K_{(1)})\\
\alpha &\longmapsto (f(\theta_K) \mapsto f^{\alpha}(\theta_K) \mid f(\tau) \in \mathcal{F}_N \text{ is finite at } \theta_K)
\end{aligned}$$

is an isomorphism.

(ii) *The map of* (i) *induces an isomorphism*

$$\{tI_2 \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) \mid t \in (\mathbb{Z}/N\mathbb{Z})^*\}/\{\pm I_2\} \longrightarrow \mathrm{Gal}(K_{(N)}/H_{\mathcal{O}}).$$

(iii) *If M is a divisor of N, then we get an isomorphism*

$$\begin{aligned}
\{tI_2 \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) \mid t \in (\mathbb{Z}/N\mathbb{Z})^* \text{ with } t \equiv \pm 1 \pmod{M}\}/\{\pm I_2\}&\\
\longrightarrow \mathrm{Gal}(K_{(N)}/K_{(M)}H_{\mathcal{O}}).&
\end{aligned}$$

Proof. (i) See Section 3 in [20].
(ii) See Proposition 5.3 in [14].
(iii) This is a direct consequence of (i) and (ii). $\square$

Lemma 3.5. *Let $N \geq 2$ be an integer for which $(N) = N\mathcal{O}_K$ is not a power of a prime ideal.*

(i) *$g_{\left[\begin{smallmatrix}0\\1/N\end{smallmatrix}\right]}(\theta_K)^{12N}$ is a unit of $\mathcal{O}_{K_{(N)}}$.*

(ii) *If u is an integer prime to N, then $g_{\left[\begin{smallmatrix}0\\u/N\end{smallmatrix}\right]}(\theta_K)^{12N}$ is also a unit of $\mathcal{O}_{K_{(N)}}$.*

Proof. (i) See Remark 4.3 in [13] and [17] (or p. 293 in [16]).

(ii) We obtain

$$\begin{aligned} g_{\left[\begin{smallmatrix}0\\u/N\end{smallmatrix}\right]}(\theta_K)^{12N} &= g_{{}^t(uI_2)\left[\begin{smallmatrix}0\\1/N\end{smallmatrix}\right]}(\theta_K)^{12N} \\ &= (g_{\left[\begin{smallmatrix}0\\1/N\end{smallmatrix}\right]}(\tau)^{12N})^{uI_2}(\theta_K) \quad \text{(by Lemma 2.3 (i) and (ii))} \\ &= (g_{\left[\begin{smallmatrix}0\\1/N\end{smallmatrix}\right]}(\theta_K)^{12N})^{uI_2} \quad \text{(by Lemmas 3.1 (i) and 3.4 (i))}. \end{aligned}$$

Now, the result follows from (i). □

Remark 3.6. The singular value $g_{\left[\begin{smallmatrix}0\\1/N\end{smallmatrix}\right]}(\theta_K)^{12N}$ is called a *Siegel–Ramachandra invariant* modulo (N), and it forms a normal basis for $K_{(N)}/K$ (see [13]).

4. Construction of relative power integral bases

We are ready to prove our main theorem concerning relative power integral bases.

Theorem 4.1. *Let K be an imaginary quadratic field not equal to $\mathbb{Q}(\sqrt{-1})$ or $\mathbb{Q}(\sqrt{-3})$. Consider integers $m \geq 2$ and $n > 0$ such that*

(i) *m has at least two prime factors,*

(ii) *each prime factor of mn splits in $K/\mathbb{Q}$.*

If $L = K_{(mn)}$ and $F = K_{(m)}H_{\mathcal{O}}$ with $\mathcal{O}$ the order of conductor mn of K, then $h_{m,n}(\theta_K)$ forms a relative power integral basis for L/F.

Proof. Let $\alpha = h_{m,n}(\theta_K)$. Since α is a unit of $\mathcal{O}_L$ by Proposition 3.3, we have the inclusion

$$\mathcal{O}_L \supseteq \mathcal{O}_F[\alpha].$$

For the converse, let β be an element of $\mathcal{O}_L$. Since $L = F(\alpha)$ by Proposition 3.3, we can express β as

$$\beta = c_0 + c_1\alpha + \cdots + c_{\ell-1}\alpha^{\ell-1} \quad \text{for some } c_0, c_1, \ldots, c_{\ell-1} \in F, \tag{4.1}$$

where $\ell = [L : F]$. In order to prove the converse inclusion $\mathcal{O}_L \subseteq \mathcal{O}_F[\alpha]$ it suffices to show that $c_0, c_1, \ldots, c_{\ell-1} \in \mathcal{O}_F$. Multiplying both sides of (4.1) by α^k $(k = 0, 1, \ldots, \ell - 1)$ yields

$$c_0\alpha^k + c_1\alpha^{k+1} + \cdots + c_{\ell-1}\alpha^{k+\ell-1} = \beta\alpha^k.$$

Now, we take the trace $\mathrm{Tr} = \mathrm{Tr}_{L/F}$ to obtain

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

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

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

Since $\alpha, \beta \in \mathcal{O}_L$, all the entries of T and $\begin{bmatrix} \mathrm{Tr}(\beta) \\ \mathrm{Tr}(\beta\alpha) \\ \vdots \\ \mathrm{Tr}(\beta\alpha^{\ell-1})\end{bmatrix}$ lie in $\mathcal{O}_F$. Hence we get

$$c_0, c_1, \ldots, c_{\ell-1} \in \frac{1}{\det(T)}\mathcal{O}_F.$$

Let $\alpha_1, \alpha_2, \ldots, \alpha_\ell$ be the conjugates of α via $\mathrm{Gal}(L/F)$. We then derive that

$$\begin{aligned}
\det(T) &= \begin{vmatrix} \sum_{k=1}^{\ell}\alpha_k^0 & \sum_{k=1}^{\ell}\alpha_k^1 & \cdots & \sum_{k=1}^{\ell}\alpha_k^{\ell-1} \\ \sum_{k=1}^{\ell}\alpha_k^1 & \sum_{k=1}^{\ell}\alpha_k^2 & \cdots & \sum_{k=1}^{\ell}\alpha_k^{\ell} \\ \vdots & \vdots & \ddots & \vdots \\ \sum_{k=1}^{\ell}\alpha_k^{\ell-1} & \sum_{k=1}^{\ell}\alpha_k^{\ell} & \cdots & \sum_{k=1}^{\ell}\alpha_k^{2\ell-2}\end{vmatrix} \\
&= \begin{vmatrix} \alpha_1^0 & \alpha_2^0 & \cdots & \alpha_\ell^0 \\ \alpha_1^1 & \alpha_2^1 & \cdots & \alpha_\ell^1 \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{\ell-1} & \alpha_2^{\ell-1} & \cdots & \alpha_\ell^{\ell-1}\end{vmatrix} \cdot \begin{vmatrix} \alpha_1^0 & \alpha_1^1 & \cdots & \alpha_1^{\ell-1} \\ \alpha_2^0 & \alpha_2^1 & \cdots & \alpha_2^{\ell-1} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_\ell^0 & \alpha_\ell^1 & \cdots & \alpha_\ell^{\ell-1}\end{vmatrix} \\
&= \prod_{1\le k_1<k_2\le\ell}(\alpha_{k_1}-\alpha_{k_2})^2 \quad \text{(by the Vandermonde determinant formula)} \\
&= \pm\prod_{\sigma_1\ne\sigma_2\in\mathrm{Gal}(L/F)}(\alpha^{\sigma_1}-\alpha^{\sigma_2}) \\
&= \pm\prod_{\sigma_1\ne\sigma_2\in\mathrm{Gal}(L/F)}(\alpha^{\sigma_1\sigma_2^{-1}}-\alpha)^{\sigma_2}.
\end{aligned} \tag{4.2}$$

If σ is a nonidentity element of $\mathrm{Gal}(L/F)$, then by Lemma 3.4 (iii) one can set $\sigma = tI_2$ for some $t \in \mathbb{N}$ such that

$$\gcd(t, mn) = 1, \quad t \equiv \pm 1 \pmod{m} \quad \text{and} \quad t \not\equiv \pm 1 \pmod{mn}.$$

Thus we deduce that

$$\begin{aligned}
\alpha^\sigma - \alpha &= h_{m,n}(\theta_K)^\sigma - h_{m,n}(\theta_K)\\
&= \left(\frac{f_{\left[\begin{smallmatrix}0\\1/mn\end{smallmatrix}\right]}(\theta_K) - f_{\left[\begin{smallmatrix}1/m\\0\end{smallmatrix}\right]}(\theta_K)}{f_{\left[\begin{smallmatrix}0\\1/m\end{smallmatrix}\right]}(\theta_K) - f_{\left[\begin{smallmatrix}1/m\\0\end{smallmatrix}\right]}(\theta_K)}\right)^\sigma - \frac{f_{\left[\begin{smallmatrix}0\\1/mn\end{smallmatrix}\right]}(\theta_K) - f_{\left[\begin{smallmatrix}1/m\\0\end{smallmatrix}\right]}(\theta_K)}{f_{\left[\begin{smallmatrix}0\\1/m\end{smallmatrix}\right]}(\theta_K) - f_{\left[\begin{smallmatrix}1/m\\0\end{smallmatrix}\right]}(\theta_K)} \quad \text{(by (2.3))}\\
&= \frac{f_{{}^t\sigma\left[\begin{smallmatrix}0\\1/mn\end{smallmatrix}\right]}(\theta_K) - f_{\left[\begin{smallmatrix}1/m\\0\end{smallmatrix}\right]}(\theta_K)}{f_{\left[\begin{smallmatrix}0\\1/m\end{smallmatrix}\right]}(\theta_K) - f_{\left[\begin{smallmatrix}1/m\\0\end{smallmatrix}\right]}(\theta_K)} - \frac{f_{\left[\begin{smallmatrix}0\\1/mn\end{smallmatrix}\right]}(\theta_K) - f_{\left[\begin{smallmatrix}1/m\\0\end{smallmatrix}\right]}(\theta_K)}{f_{\left[\begin{smallmatrix}0\\1/m\end{smallmatrix}\right]}(\theta_K) - f_{\left[\begin{smallmatrix}1/m\\0\end{smallmatrix}\right]}(\theta_K)}\\
&\qquad\qquad \text{(by Lemmas 3.4 (iii) and 2.2)}\\
&= \frac{f_{\left[\begin{smallmatrix}0\\t/mn\end{smallmatrix}\right]}(\theta_K) - f_{\left[\begin{smallmatrix}0\\1/mn\end{smallmatrix}\right]}(\theta_K)}{f_{\left[\begin{smallmatrix}0\\1/m\end{smallmatrix}\right]}(\theta_K) - f_{\left[\begin{smallmatrix}1/m\\0\end{smallmatrix}\right]}(\theta_K)}\\
&= \frac{\wp_{\left[\begin{smallmatrix}0\\t/mn\end{smallmatrix}\right]}(\theta_K) - \wp_{\left[\begin{smallmatrix}0\\1/mn\end{smallmatrix}\right]}(\theta_K)}{\wp_{\left[\begin{smallmatrix}0\\1/m\end{smallmatrix}\right]}(\theta_K) - \wp_{\left[\begin{smallmatrix}1/m\\0\end{smallmatrix}\right]}(\theta_K)} \quad \text{(by Definition (2.1))}\\
&= \frac{g_{\left[\begin{smallmatrix}0\\(t+1)/mn\end{smallmatrix}\right]}(\theta_K)g_{\left[\begin{smallmatrix}0\\(t-1)/mn\end{smallmatrix}\right]}(\theta_K)g_{\left[\begin{smallmatrix}0\\1/m\end{smallmatrix}\right]}(\theta_K)^2 g_{\left[\begin{smallmatrix}1/m\\0\end{smallmatrix}\right]}(\theta_K)^2}{g_{\left[\begin{smallmatrix}1/m\\1/m\end{smallmatrix}\right]}(\theta_K)g_{\left[\begin{smallmatrix}-1/m\\1/m\end{smallmatrix}\right]}(\theta_K)g_{\left[\begin{smallmatrix}0\\t/mn\end{smallmatrix}\right]}(\theta_K)^2 g_{\left[\begin{smallmatrix}0\\1/mn\end{smallmatrix}\right]}(\theta_K)^2} \quad \text{(by Lemma 2.4).}
\end{aligned}$$

Since each of

$$\begin{bmatrix}0\\1/m\end{bmatrix}, \begin{bmatrix}1/m\\0\end{bmatrix}, \begin{bmatrix}1/m\\1/m\end{bmatrix}, \begin{bmatrix}-1/m\\1/m\end{bmatrix}, \begin{bmatrix}0\\t/mn\end{bmatrix}, \begin{bmatrix}0\\1/mn\end{bmatrix}$$

has by the hypothesis (i) primitive denominator with at least two prime factors, the values

$$g_{\left[\begin{smallmatrix}0\\1/m\end{smallmatrix}\right]}(\theta_K), g_{\left[\begin{smallmatrix}1/m\\0\end{smallmatrix}\right]}(\theta_K), g_{\left[\begin{smallmatrix}1/m\\1/m\end{smallmatrix}\right]}(\theta_K), g_{\left[\begin{smallmatrix}-1/m\\1/m\end{smallmatrix}\right]}(\theta_K), g_{\left[\begin{smallmatrix}0\\t/mn\end{smallmatrix}\right]}(\theta_K), g_{\left[\begin{smallmatrix}0\\1/mn\end{smallmatrix}\right]}(\theta_K)$$

are units as algebraic integers by Lemmas 2.3 (iii) and 3.2. On the other hand, set

$$\frac{t+1}{mn} = \frac{a}{N} \quad \text{for some relatively prime positive integers } N \text{ and } a.$$

Since $t \not\equiv \pm 1 \pmod{mn}$, we get $N \geq 2$. Moreover, $(N) = N\mathcal{O}_K$ is not a power of a prime ideal by the hypothesis (ii). So $g_{\left[\begin{smallmatrix}0\\(t+1)/mn\end{smallmatrix}\right]}(\theta_K) = g_{\left[\begin{smallmatrix}0\\a/N\end{smallmatrix}\right]}(\theta_K)$ is a unit as an algebraic integer by Lemma 3.5 (ii). In a similar fashion, we also see that $g_{\left[\begin{smallmatrix}0\\(t-1)/mn\end{smallmatrix}\right]}(\theta_K)$ is a unit as an algebraic integer. Therefore $\alpha^\sigma - \alpha$ is a unit of $\mathcal{O}_L$. This implies that $\det(T)$ is a unit of $\mathcal{O}_F$ by (4.2), and hence we get the converse inclusion

$$\mathcal{O}_L \subseteq \mathcal{O}_F[\alpha]$$

as desired. □

Remark 4.2. Since $\mathcal{O}_L = \mathcal{O}_F[\alpha]$ and the discriminant of α is a unit of $\mathcal{O}_F$, L/F is an unramified extension.

References

[1] Gaál, I. and Schulte, N.: Computing all power integral bases of cubic fields. *Math. Comp.* **53** (1989), no. 188, 689–696.

[2] Gaál, I.: Power integral bases in orders of families of quartic fields. *Publ. Math. Debrecen* **42** (1993), no. 3-4, 253–263.

[3] Gaál, I.: Computing elements of given index in totally complex cyclic sextic fields. *J. Symbolic Comput.* **20** (1995), no. 1, 61–69.

[4] Gaál, I.: Computing all power integral bases in orders of totally real cyclic sextic number fields. *Math. Comp.* **65** (1996), no. 214, 801–822.

[5] Gaál, I. and Pohst, M.: On the resolution of index form equations in sextic fields with an imaginary quadratic subfield. *J. Symbolic Comput.* **22** (1996), no. 4, 425–434.

[6] Gaál, I. and Pohst, M.: Power integral bases in a parametric family of totally real cyclic quintics. *Math. Comp.* **66** (1997), no. 220, 1689–1696.

[7] Gaál, I. and Győry, K.: Index form equations in quintic fields. *Acta Arith.* **89** (1999), no. 4, 379–396.

[8] Gaál, I.: Power integer bases in algebraic number fields. *Ann. Univ. Sci. Budapest. Sect. Comput.* **18** (1999), 61–87.

[9] Gaál, I.: Solving index form equations in fields of degree 9 with cubic subfields. *J. Symbolic Comput.* **30** (2000), no. 2, 181–193.

[10] Gaál, I. and Pohst, M.: Computing power integral bases in quartic relative extensions. *J. Number Theory* **85** (2000), no. 2, 201–219.

[11] Gaál, I.: Power integral bases in cubic relative extensions. *Experiment. Math.* **10** (2001), no. 1, 133–139.

[12] Gaál, I. and Szabó, T.: Power integral bases in parametric families of biquadratic fields. *JP J. Algebra Number Theory Appl.* **24** (2012), no. 1, 105–114.

[13] Jung, H. Y., Koo, J. K. and Shin, D. H.: Normal bases of ray class fields over imaginary quadratic fields. *Math. Z.* **271** (2012), no. 1-2, 109–116.

[14] Koo, J. K. and Shin, D. H.: Function fields of certain arithmetic curves and application. *Acta Arith.* **141** (2010), no. 4, 321–334.

[15] Kubert, D. and Lang, S.: *Modular units.* Grundlehren der mathematischen Wissenschaften 244, Spinger-Verlag, New York-Berlin, 1981.

[16] Lang, S.: *Elliptic functions.* Second edition. Graduate Texts in Mathematics 112, Spinger-Verlag, New York, 1987.

[17] Ramachandra, K.: Some applications of Kronecker's limit formula. *Ann. of Math. (2)* **80** (1964), 104–148.

[18] Shimura, G.: *Introduction to the arithmetic theory of automorphic functions.* Iwanami Shoten, Publishers, Tokyo; Princeton University Press, Princeton, NJ, 1971.

[19] Silverman, J. H.: *The arithmetic of elliptic curves.* Graduate Texts in Mathematics 106, Springer-Verlag, New York, 1992.

[20] Stevenhagen, P.: Hilbert's 12th problem, complex multiplication and Shimura reciprocity. In *Class field theory – its centenary and prospect (Tokyo, 1998),* 161–176. Adv. Stud. Pure Math. 30, Math. Soc. Japan, Tokyo, 2001.

[21] WASHINGTON, L. C.: *Introduction to cyclotomic fields.* Second edition. Graduate Texts in Mathematics 83, Springer-Verlag, New York, 1997.

Received January 21, 2013.

HO YUN JUNG: National Institute for Mathematical Sciences, Daejeon 305-811, Republic of Korea.
E-mail: hoyunjung@nims.re.kr

JA KYUNG KOO: Department of Mathematical Sciences, KAIST, Daejeon 305-701, Republic of Korea.
E-mail: 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.
E-mail: dhshin@hufs.ac.kr

The third named (corresponding) author was supported by the Hankuk University of Foreign Studies Research Fund of 2014.