Generators for abelian extensions of number fields

JA KYUNG KOO AND DONG HWA SHIN

Abstract

Let \( U/L \) be a finite abelian extension of number fields. We first construct a universal primitive generator of \( U \) over \( L \) whose relative trace to any intermediate field \( F \) becomes a generator of \( F \) over \( L \), too. We also develop a similar argument in terms of norm. As its examples we investigate towers of ray class fields over imaginary quadratic fields. And, we further present a new method of finding a normal element for the extension \( U/L \).

1 Introduction

Let \( U/L \) be a finite abelian extension of number fields. If \( F \) is an intermediate field of \( U/L \), then it is also an abelian extension of \( L \) by Galois theory. Furthermore, we have a primitive generator of \( F \) over \( L \) by the primitive element theorem (see also [6, Theorems 8.2 or 8.4]). In this paper we shall first show that there exists a universal generator \( \alpha \) of \( U \) over \( L \) for which its relative trace \( \Tr_{U/F}(\alpha) \) becomes a generator of \( F \) over \( L \) (Theorem 2.2), too. And, for a field tower \( L = F_0 \leq F_1 \leq F_2 \leq \cdots \leq F_t = U \) we shall also construct an element \( \beta \) of \( U \) whose relative norm \( N_{U/F_k}(\beta) \) generates \( F_k \) over \( L \) for each index \( 1 \leq k \leq t \) (Theorem 4.2).

Let \( K \) be an imaginary quadratic field other than \( \mathbb{Q}(\sqrt{-1}) \) and \( \mathbb{Q}(\sqrt{-3}) \). For a nonzero integral ideal \( \mathfrak{f} \) of \( K \), we denote by \( K_\mathfrak{f} \) the ray class field of \( K \) modulo \( \mathfrak{f} \). Let \( p \) be an odd prime and \( n (\geq 2) \) be an integer. Then it is well-known ([8, Chapter 10, Corollary to Theorem 7]) that \( K_{(p^n)} \) is generated by the special value of a Fricke function over \( K_{(p)} \). As one example of Theorem 2.2 we shall construct a generator \( \alpha \) of \( K_{(p^n)} \) over \( K_{(p)} \) whose

2010 Mathematics Subject Classification. Primary 12F05, Secondary 11G16.

Key words and phrases. Abelian extensions, class fields, normal bases, primitive element theorem.

The first author was partially supported by the NRF of Korea grant funded by MISP (2013042157).

*The corresponding author was supported by Hankuk University of Foreign Studies Research Fund of 2013.
relative trace $\text{Tr}_{K(p^m)/K(p)}(\alpha)$ also generates $K(p^m)$ over $K(p)$ for each integer $2 \leq m \leq n$ (Theorem 3.5). And, let $N_1, N_2, \ldots, N_t$ ($t \geq 1$) be a sequence of integers such that $N_1 \geq 2$ and $N_1|N_2|\cdots|N_t$. As for another example of Theorem 4.2 we shall construct an element $\beta$ of $K(N_t)$ whose relative norm $N_{K(N_t)/K(N_k)}(\beta)$ generates $K(N_k)$ over $K$ for each index $1 \leq k \leq t$ (Example 4.3), which is relatively simpler than the work of Ramachandra ([11]).

On the other hand, the normal basis theorem ([17, §8.11]) guarantees the existence of an element $\alpha \in U$ whose Galois conjugates over $L$ form a basis for $U$ over $L$ as a vector space. We call such an element $\alpha$ a normal element for $U/L$. Although one can find a primitive generator for $U/L$, not much seems to be known until now how to construct such a normal element. For instance, Okada ([9]) constructed in 1980 a normal element of the maximal real subfield of $\mathbb{Q}(e^{2\pi i/q})$ over $\mathbb{Q}$ by extending Chowla’s work ([1]) with cotangent function. See also [10]. After Okada, Taylor ([16]) and Schertz ([12]) established Galois module structures of ring of integers of certain abelian extensions of an imaginary quadratic field and also found a normal element by making use of special value of modular function. And, Komatsu ([4]) further considered certain abelian extensions $U$ and $L$ of the cyclotomic field $\mathbb{Q}(e^{2\pi i/5})$ and constructed a normal element for $U/L$ in terms of special value of Siegel modular function. Unlike their works, however, we shall present a relatively simple new formula of constructing a normal element for $U/L$ by using a lemma developed in [3] which can be deduced from the Frobenius determinant relation (Theorem 5.3).

2 Generators from relative traces

First, we shall present a simple lemma.

**Lemma 2.1.** Given a sequence of $\ell$ ($\geq 1$) nonnegative integers

$$N_1, N_2, \ldots, N_\ell,$$

we can construct a sequence of $\ell$ positive integers

$$M_1, M_2, \ldots, M_\ell$$

in view of $N_1, N_2, \ldots, N_\ell$ such that

(i) $M_i \geq 1 + N_i$ for each index $1 \leq i \leq \ell$,

(ii) $\gcd(M_i, N_i) = 1$ for every index $1 \leq i \leq \ell$,

(iii) $\gcd(M_i, M_j) = 1$ whenever $i \neq j$. 

Proof. Set $M_0 = 1$ and
\[
M_i = 1 + N_i \prod_{k=0}^{i-1} M_k \quad (1 \leq i \leq \ell).
\]
Since $M_0 = 1$ and $N_i \geq 0$, the recursive formula (1) yields the property (i). Furthermore, the relation
\[
M_i - N_i \prod_{k=0}^{i-1} M_k = 1
\]
induced directly from (1) enables us to have the properties (ii) and (iii).

Let $U$ be a finite abelian extension of a number field $L$ with $[U : L] \geq 2$. Let
\[L < F_1, F_2, \ldots, F_\ell \leq U\]
be (all of) its intermediate subfields properly containing $L$. Since $U/L$ is an abelian extension, so is $F_i/L$ ($1 \leq i \leq \ell$) by Galois theory. Furthermore, there is a nonzero algebraic integer $\alpha_i$ that generates $F_i$ over $L$ by the primitive element theorem. We set
\[
N = [U : L] \prod_{i=1}^{\ell} |N_{L/Q}(\text{disc}(\alpha_i, F_i/L))|,
\]
which is a positive integer, and take
\[
M_0 = 1 \quad \text{and} \quad M_i = 1 + N \prod_{k=0}^{i-1} M_k \quad (1 \leq i \leq \ell).
\]
Then the sequence $M_1, M_2, \ldots, M_\ell$ satisfies the properties (i)~(iii) in Lemma 2.1 with $N_i = N$ ($1 \leq i \leq \ell$). Now we consider the element
\[
\alpha = \sum_{i=1}^{\ell} \frac{\alpha_i}{M_i} \in U.
\]

**Theorem 2.2.** The relative trace
\[
\text{Tr}_{U/F_i}(\alpha)
\]
generates $F_i$ over $L$ for each index $1 \leq i \leq \ell$.

Proof. On the contrary, suppose that $\text{Tr}_{U/F_j}(\alpha)$ does not generates $F_j$ over $L$ for some index $1 \leq j \leq \ell$. Then there is an element $\rho \in \text{Gal}(F_j/L)$ with $\rho \neq \text{id}$ fixing $\text{Tr}_{U/F_j}(\alpha)$. We then obtain by the definition (2) and the fact $\text{Tr}_{U/F_j}(\alpha) = \text{Tr}_{U/F_j}(\alpha)$ that
\[
\frac{T_{U/F_j}(\alpha_j)}{M_j} + \sum_{1 \leq i \leq \ell, i \neq j} \frac{T_{U/F_i}(\alpha_i)}{M_i} = \frac{T_{U/F_j}(\alpha_j)}{M_j} + \sum_{1 \leq i \leq \ell, i \neq j} \frac{T_{U/F_i}(\alpha_i)}{M_i}.
\]
And, we further derive that
\[
\sum_{1 \leq i \leq \ell, i \neq j} \frac{1}{M_i}(\text{Tr}_{U/F_j}(\alpha_i)^\rho - \text{Tr}_{U/F_j}(\alpha_i)) = \frac{1}{M_j}(\text{Tr}_{U/F_j}(\alpha_j) - \text{Tr}_{U/F_j}(\alpha_j)^\rho) = \frac{1}{M_j}[U : F_j](\alpha_j - \alpha_j^\rho)
\]
because \(\alpha_j \in F_j\).

Multiplying both sides by \(M_1M_2 \cdots M_\ell\) we get
\[
M_j \sum_{1 \leq i \leq \ell, i \neq j} \frac{M_1M_2 \cdots M_\ell}{M_iM_j}(\text{Tr}_{U/F_j}(\alpha_i)^\rho - \text{Tr}_{U/F_j}(\alpha_i)) = \frac{M_1M_2 \cdots M_\ell}{M_j}[U : F_j](\alpha_j - \alpha_j^\rho).
\]

Here, we note that the left hand side is an algebraic integer divisible by an integer \(M_j (\geq 2)\), whereas the right hand side is a nonzero algebraic integer prime to \(M_j\) because \(\rho \neq \text{id}, \gcd(M_j, N) = 1\) and \(\gcd(M_i, M_j) = 1\) if \(i \neq j\). This yields a contradiction.

Therefore, we conclude that \(\text{Tr}_{U/F_i}(\alpha)\) generates \(F_i\) over \(L\) for each index \(1 \leq i \leq \ell\). \(\square\)

**Remark 2.3.** We can replace \(N\) by any positive integer divisible by all prime factors of \(N\).

### 3 Towers of class fields

For each positive integer \(N\) let \(\mathcal{F}_N\) be the field of all meromorphic modular functions of level \(N\) whose Fourier coefficients belong to \(\mathbb{Q}(\zeta_N)\) with \(\zeta_N = e^{2\pi i/N}\). As is well-known [13, §6.2] the elliptic modular function \(j\) generates \(\mathcal{F}_1\) over \(\mathbb{Q}\), and \(\mathcal{F}_N\) is a Galois extension of \(\mathcal{F}_1\) whose Galois group is isomorphic to \(\text{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I_2\}\).

For a lattice \(\Lambda = [\tau_1, \tau_2]\) in \(\mathbb{C}\), the **Weierstrass \(\wp\)-function** relative to \(\Lambda\) is defined by
\[
\wp(z; \Lambda) = \frac{1}{z^2} + \sum_{\omega \in \Lambda - \{0\}} \left\{ \frac{1}{(z - \omega)^2} - \frac{1}{\omega^2} \right\} \quad (z \in \mathbb{C}).
\]

Let \(N (\geq 2)\) be an integer and \([r, s] \in (1/N)\mathbb{Z}^2 - \mathbb{Z}^2\). We define the **Fricke function** \(f_{[r]}(\tau)\) by
\[
f_{[r]}(\tau) = \frac{g_2(\tau)g_3(\tau)}{g_2(\tau)^3 - 27g_3(\tau)^2}\wp_{[r]}(\tau) \quad (\tau \in \mathbb{H}),
\]
where
\[
g_k(\tau) = 60 \sum_{\omega \in [\tau, 1] - \{0\}} \frac{1}{\omega^{2k}} \quad (k = 2, 3) \quad \text{and} \quad \wp_{[r]}(\tau) = \wp(r\tau + s; [\tau, 1]).
\]
Furthermore, we define the Siegel function $g_{[r_s]}(\tau)$ by

$$g_{[r_s]}(\tau) = -q^{(1/2)(r^2-r+1/6)}e^{\pi is(r-1)}(1 - q^r e^{2\pi is})(1 - q^{n+r} e^{-2\pi is}),$$

where $q = e^{2\pi ir}$. Observe that it has neither zeros nor poles on $\mathbb{H}$. Then, $f_{[r_s]}(\tau)$ and $g_{[r_s]}(\tau)^{12N}$ belong to $\mathcal{F}_N$ and satisfy the transformation rules

$$(4) \quad f_{[r_s]}(\tau)^\gamma = f_{[\gamma [r_s]]}(\tau) \quad \text{and} \quad (g_{[r_s]}(\tau)^{12N})^\gamma = g_{[\gamma [r_s]]}(\tau)^{12N}$$

, respectively, for all $\gamma \in \text{Gal}(\mathcal{F}_N/\mathcal{F}_1) \simeq \text{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I_2\}$ ([8, Chapter 6, §2–3] and [3, Proposition 3.4]).

**Lemma 3.1.** Let $\left[ \begin{array}{c} r_1 \\ s_1 \end{array} \right]$, $\left[ \begin{array}{c} r_2 \\ s_2 \end{array} \right] \in (1/N)\mathbb{Z}^2 - \mathbb{Z}^2$ for an integer $N \geq 2$ such that $\left[ \begin{array}{c} r_1 \\ s_1 \end{array} \right] \neq \pm \left[ \begin{array}{c} r_2 \\ s_2 \end{array} \right] \pmod{\mathbb{Z}^2}$. Then we have the relation

$$\wp_{[r_1/s_1]}(\tau) - \wp_{[r_2/s_2]}(\tau) = -\frac{g_{[r_1+r_2/s_1+s_2]}(\tau)g_{[r_1-r_2/s_1-s_2]}(\tau)\eta(\tau)^4}{g_{[r_1/s_1]}(\tau)^2g_{[r_2/s_2]}(\tau)^2},$$

where

$$\eta(\tau) = \sqrt{2\pi} \varsigma_8 q^{1/24} \prod_{n=1}^{\infty} (1 - q^n).$$

**Proof.** See [7, p.51].

Let $K$ be an imaginary quadratic field of discriminant $d_K$. We set

$$(5) \quad \theta_K = \frac{d_K + \sqrt{d_K}}{2},$$

and denote by $H_K$ and $K_{(N)}$ the Hilbert class field of $K$ and the ray class field of $K$ modulo $(N)$ for a positive integer $N$, respectively.

**Lemma 3.2.** Let $N \geq 2$. By the main theorem of complex multiplication we have the followings.

(i) $H_K = K(j(\theta_K)).$

(ii) $K_{(N)} = K(h(\theta_K) | h \in \mathcal{F}_N$ is finite at $\theta_K).$

(iii) If $K \neq \mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-3})$, then $K_{(N)} = H_K(f_{[0/1]}(\theta_K)) = K(g_{[0/1]}(\theta_K)^{12Nn})$ for any nonzero integer $n$. 

5
Proof. (i) See [8, Chapter 10, Theorem 1] or [13, Theorem 5.7].

(ii) See [8, Chapter 10, Corollary to Theorem 2].

(iii) See [8, Chapter 10, Corollary to Theorem 7] and [3, Theorem 4.2].

In what follows we let \( K \neq \mathbb{Q}((\sqrt{-1}), \mathbb{Q}((\sqrt{-3})) \) until \( \S 5 \).

Lemma 3.3 (Shimura’s reciprocity law). Let \( N \geq 2 \) and let \( x^2 + Bx + C \in \mathbb{Z}[x] \) be the minimal polynomial of \( \theta_K \) over \( \mathbb{Q} \). Then the matrix group

\[
W_{K,N} = \left\{ \begin{bmatrix} u-Bv & -Cv \\ v & u \end{bmatrix} \in \text{GL}_2(\mathbb{Z}/N\mathbb{Z}) \mid u, v \in \mathbb{Z}/N\mathbb{Z} \right\}
\]

gives rise to the isomorphism

\[
W_{K,N}/\{\pm I_2\} \rightarrow \text{Gal}(K(N)/H_K)
\]

\[
\alpha \mapsto (h(\theta_K) \mapsto h^\alpha(\theta_K) \mid h \in \mathcal{F}_N \text{ is finite at } \theta_K).
\]

Proof. See [15, §3].

Let \( p \) be an odd prime and let \( n (\geq 2) \) be an integer. We then have a tower of ray class fields

\[
K_{(p)} < K_{(p^2)} < \cdots < K_{(p^n)}
\]

with

\[
[K_{(p^{m+1})} : K_{(p^m)}] = p^2 \quad (1 \leq m \leq n - 1)
\]

[7, Chapter VI, Theorem 1].

For each positive integer \( m \) we define a function

\[
f_m(\tau) = p^{2(m+1)} \frac{f_{[0/1/p^m]}(\tau) - f_{[0/1/p]}(\tau)}{f_{[0/1/p]}(\tau) - f_{[0/1/p]}(\tau)}
\]

that belongs to \( \mathcal{F}_{p^m} \).

Lemma 3.4. Let \( \left[ \begin{array}{c} r \\ s \end{array} \right] \in (1/N)\mathbb{Z}^2 - \mathbb{Z}^2 \) for an integer \( N (\geq 2) \). Then we get the followings:

(i) \( g_{[r/s]}(\theta_K) \) and \( Ng_{[r/s]}(\theta_K)^{-1} \) are algebraic integers dividing \( N \).

(ii) \( f_m(\theta_K) \) is an algebraic integer which generates \( K_{(p^m)} \) over \( K_{(p)} \).
(iii) \(|N_{K(p)/Q}(\text{disc}(f_m(\theta_K), K_{(p^m)/K(p)}))|\) is a power of \(p\).

**PROOF.**

(i) See [51 §3] and [7] p.45, Example.

(ii) Since \(K(p) = H_K(f_{\begin{align} & 0 \\ & 1/p \end{align}}(\theta_K))\) and \(K_{(p^m)} = H_K(f_{\begin{align} & 0 \\ & 1/\text{p^m} \end{align}}(\theta_K))\) by Lemma 3.2(iii), we achieve from the definition \(\text{Lemma 7}\)

\[K_{(p^m)} = K(p)(f_m(\theta_K)).\]

On the other hand, we obtain by definition \(\text{Lemma 3}\) and Lemma 3.1 that

\[f_m(\theta_K) = g_{\begin{align} & 1/p \\ & 1/\text{p^m} \end{align}}(\theta_K)g_{\begin{align} & -1/p \\ & 1/\text{p^m} \end{align}}(\theta_K)g_{\begin{align} & 0 \\ & 1/p \end{align}}(\theta_K)^2 \]

\[\times (pg_{\begin{align} & 1/p \\ & 1/\text{p^m} \end{align}}(\theta_K)^{-1})\]

\[\times (pg_{\begin{align} & -1/p \\ & 1/\text{p^m} \end{align}}(\theta_K)^{-1})\]

\[\times (p^{2m}g_{\begin{align} & 0 \\ & 1/\text{p^m} \end{align}}(\theta_K)^{-2}),\]

which yields that \(f_m(\theta_K)\) is an algebraic integer by (i).

(iii) Let \(\sigma \in \text{Gal}(K_{(p^m)/K(p)})\) with \(\sigma \neq \text{id}\). By Lemma 3.3 we may identify \(\sigma\) with an element \(\begin{bmatrix} u-Bv & -Cu \\ v & u \end{bmatrix}\) of \(\text{GL}_2(\mathbb{Z}/p^m\mathbb{Z})\), where \(\text{min}(\theta_K, \mathbb{Q}) = x^2 + Bx + C\). We then see that

\[f_m(\theta_K)^\sigma - f_m(\theta_K) = p^{2(m+1)}\left(\frac{f_{\begin{align} & 0 \\ & 1/p \end{align}}(\theta_K) - f_{\begin{align} & 0 \\ & 1/\text{p^m} \end{align}}(\theta_K)}{f_{\begin{align} & 0 \\ & 1/p \end{align}}(\theta_K) - f_{\begin{align} & 0 \\ & 1/\text{p^m} \end{align}}(\theta_K)}\right)^\sigma - \frac{f_{\begin{align} & 0 \\ & 1/p \end{align}}(\theta_K) - f_{\begin{align} & 0 \\ & 1/\text{p^m} \end{align}}(\theta_K)}{f_{\begin{align} & 0 \\ & 1/p \end{align}}(\theta_K) - f_{\begin{align} & 0 \\ & 1/\text{p^m} \end{align}}(\theta_K)}\]

by the definition \(\text{Lemma 7}\)

\[= p^{2(m+1)}\left(\frac{f_{\begin{align} & 0 \\ & 1/p \end{align}}(\theta_K)^\sigma - f_{\begin{align} & 0 \\ & 1/\text{p^m} \end{align}}(\theta_K)}{f_{\begin{align} & 0 \\ & 1/p \end{align}}(\theta_K) - f_{\begin{align} & 0 \\ & 1/\text{p^m} \end{align}}(\theta_K)}\right) - \frac{f_{\begin{align} & 0 \\ & 1/p \end{align}}(\theta_K) - f_{\begin{align} & 0 \\ & 1/\text{p^m} \end{align}}(\theta_K)}{f_{\begin{align} & 0 \\ & 1/p \end{align}}(\theta_K) - f_{\begin{align} & 0 \\ & 1/\text{p^m} \end{align}}(\theta_K)}\]

because \(\sigma\) leaves \(K(p)\) fixed

\[= p^{2(m+1)}\frac{f_{\begin{align} & 0 \\ & 1/p \end{align}}(\theta_K)^\sigma - f_{\begin{align} & 0 \\ & 1/\text{p^m} \end{align}}(\theta_K)}{f_{\begin{align} & 0 \\ & 1/p \end{align}}(\theta_K) - f_{\begin{align} & 0 \\ & 1/\text{p^m} \end{align}}(\theta_K)}\]

by Lemma 3.3 and \(\text{Lemma 4}\)

\[= p^{2(m+1)}\frac{f_{\begin{align} & v/p^m \\ & u/p^m \end{align}}(\theta_K)^\sigma - f_{\begin{align} & 0 \\ & 1/\text{p^m} \end{align}}(\theta_K)}{f_{\begin{align} & 0 \\ & 1/p \end{align}}(\theta_K) - f_{\begin{align} & 0 \\ & 1/\text{p^m} \end{align}}(\theta_K)}\]

by Lemma 3.1

Since \(f_m(\theta_K)\) is an algebraic integer, this value is an algebraic integer, too. Moreover, it divides a power of \(p\) by (i). Therefore, we conclude that \(|N_{K(p)/Q}(\text{disc}(f_m(\theta_K), K_{(p^m)/K(p)}))|\) is a power of \(p\).
**Theorem 3.5.** Let \( n \geq 2 \) be an integer. Set
\[
M_1 = 1 \quad \text{and} \quad M_m = 1 + p \prod_{k=1}^{m-1} M_k \quad (2 \leq m \leq n),
\]
and
\[
\alpha = \sum_{m=2}^{n} \frac{\alpha_m}{M_m} \quad \text{with} \quad \alpha_m = f_m(\theta_K).
\]
Then the relative trace
\[
\text{Tr}_{K(p^m)/K(p^n)}(\alpha)
\]
generates \( K_{(p^m)} \) over \( K_{(p^n)} \) for each integer \( 2 \leq m \leq n \).

**Proof.** Note that the positive integer
\[
[K_{(p^n)} : K_{(p)}] \prod_{2 \leq m \leq n} |N_{K_{(p^n)}/K_{(p)}}(\text{disc}(f_m(\theta_K), K_{(p^m)}/K_{(p)})|)
\]
is a power of \( p \) by (6) and Lemma 3.4(iii). Furthermore, since each \( f_m(\theta_K) \) \( (2 \leq m \leq n) \) is an algebraic integer which generates \( K_{(p^m)} \) over \( K_{(p)} \) by Lemma 3.4(ii), the assertion follows from Theorem 2.2.

\( \square \)

4 Generators from relative norms

Let \( U/L \) be a finite abelian extension of number fields, and consider a tower of fields
\[
L = F_0 \leq F_1 \leq F_2 \leq \cdots \leq F_t = U \quad (t \geq 1)
\]
with
\[
d_k = [F_k : F_{k-1}] \quad (1 \leq k \leq t).
\]
In this section we shall present an element \( \beta \) of \( U \) whose relative norm \( N_{F_k/F_k}(\beta) \) renders a generator of \( F_k \) over \( F_0 \) for each index \( 1 \leq k \leq m \). First, we need a lemma.

**Lemma 4.1.** Let \( K \) be a number field and \( \alpha \) be an algebraic integer for which \( K(\alpha) \) is Galois over \( K \). Then, any nonzero power of \( 3\alpha + 1 \) also generates \( K(\alpha) \) over \( K \).

**Proof.** Let \( n \) be a nonzero integer. Suppose on the contrary that \( K((3\alpha + 1)^n) \) is properly contained in \( K(\alpha) \). Then there exists an element \( \rho \in \text{Gal}(K(\alpha)/K) \) with \( \rho \neq \text{id} \) fixing \( (3\alpha + 1)^n \). Since \( 3\alpha + 1 \neq 0 \), we get \( 3\alpha^\rho + 1 = \zeta(3\alpha + 1) \) for some \( |n| \)-th root of unity \( \zeta \neq 0 \), from which it follows that
\[
3(\alpha^\rho - \zeta \alpha) = \zeta - 1 \quad (\neq 0).
\]
Since \( \alpha^\rho - \zeta \alpha \) is a nonzero algebraic integer, we see that

\[
(9) \quad |N_{K(\alpha)/\mathbb{Q}}(3(\alpha^\rho - \zeta \alpha))| = 3^d |N_{K(\alpha)/\mathbb{Q}}(\alpha^\rho - \zeta \alpha)| \geq 3^d
\]

where \( d = [K(\alpha) : \mathbb{Q}] \). On the other hand, since any Galois conjugate of \( \zeta - 1 \) over \( \mathbb{Q} \) is of the form \( \zeta^s - 1 \) for some integer \( s \) and \( |\zeta^s - 1| \leq |\zeta^s| + 1 = 2 \), we obtain

\[
|N_{K(\alpha)/\mathbb{Q}}(\zeta - 1)| \leq 2^d.
\]

But, this contradicts (8) and (9). Therefore we achieve the lemma.

By the primitive element theorem, there is an algebraic integer \( \beta_k \) which generates \( F_k \) over \( F_{k-1} \) for each index \( 1 \leq k \leq t \). Furthermore, we may assume that

\[
(10) \quad F_k = F_{k-1}(\beta_k^n) \quad \text{for any nonzero integer } n
\]

in the sense of Lemma 4.1

**Theorem 4.2.** With the notations as above, let

\[
\beta = \beta_1 \prod_{s=2}^{t} \frac{\beta_s^d}{N_{F_s/F_{s-1}}(\beta_s)}
\]

Then, for any nonzero integer \( n \) the relative norm

\[
N_{F_k/F_0}(\beta^n)
\]

generates \( F_k \) over \( F_0 \) for each index \( 1 \leq k \leq t \).

**Proof.** We use the induction on \( m \).

If \( t = 1 \), then we get \( \beta = \beta_1 \), and so the assertion is obvious by (10).

Now, assume that the assertion holds for \( t = \ell \) \((\geq 1)\), and consider the case where \( t = \ell + 1 \). We then deduce that

\[
N_{F_{\ell+1}/F_\ell}(\beta) = N_{F_{\ell+1}/F_\ell} \left( \beta_1 \prod_{s=2}^{\ell+1} \frac{\beta_s^{d_s}}{N_{F_s/F_{s-1}}(\beta_s)} \right)
\]

\[
= N_{F_{\ell+1}/F_\ell} \left( \beta_1 \prod_{s=2}^{\ell} \frac{\beta_s^{d_s}}{N_{F_s/F_{s-1}}(\beta_s)} \right) N_{F_{\ell+1}/F_\ell} \left( \frac{\beta^{d_{\ell+1}}_{\ell+1}}{N_{F_{\ell+1}/F_\ell}(\beta_{\ell+1})} \right)
\]

\[
= \left( \beta_1 \prod_{s=2}^{\ell} \frac{\beta_s^{d_s}}{N_{F_s/F_{s-1}}(\beta_s)} \right)^{d_{\ell+1}} N_{F_{\ell+1}/F_\ell}(\beta_{\ell+1})^{d_{\ell+1}}
\]

\[
= \left( \beta_1 \prod_{s=2}^{\ell} \frac{\beta_s^{d_s}}{N_{F_s/F_{s-1}}(\beta_s)} \right)^{d_{\ell+1}}.
\]
Thus we obtain by induction hypothesis that for each index $1 \leq k \leq \ell$

\[(11) \quad F_k = F_0(N_{F_t/F_k}(N_{F_{t+1}/F_t}(\beta))^n) = F_0(N_{F_{t+1}/F_k}(\beta)^n) \quad \text{for any nonzero integer } n.\]

On the other hand, since $F_{t+1}/F_0$ is an abelian extension, so is $F_0(\beta^n)/F_0$ by Galois theory. This fact implies that $F_0(\beta^n)$ contains $N_{F_{t+1}/F_t}(\beta)^n$, and we derive that

\[
F_0(N_{F_{t+1}/F_t}(\beta)^n) = F_0(\beta^n) = F_0(\beta^n)N_{F_{t+1}/F_t}(\beta)^n = F_t(\beta^n) \quad \text{by (11) with } k = \ell
\]

\[
= F_t\left(\beta_1 \prod_{s=2}^{t+1} \frac{\beta_s^{d_s}}{N_{F_s/F_{s-1}}(\beta_s^n)}\right) = F_t(\beta t + 1) = F_{t+1} \quad \text{by (10).}
\]

Hence the assertion is also true for $t = \ell + 1$. This complete the proof. \qed

**Example 4.3.** Let $K$ be an imaginary quadratic field other than $\mathbb{Q}(\sqrt{-1})$ and $\mathbb{Q}(\sqrt{-3})$, and let $\theta_K$ be as in (3). For a sequence of integers $N_1, N_2, \ldots, N_t$ $(t \geq 1)$ such that

\[2 \leq N_1 \quad \text{and} \quad N_1 | N_2 | \cdots | N_t,\]

consider a tower of class fields

\[K \leq K_{(N_1)} \leq K_{(N_2)} \leq \cdots \leq K_{(N_t)}.\]

For each index $1 \leq k \leq t$ and any nonzero integer $n$, the special value $g[0^{1/N_{k}}](\theta_K)^{12N_k n}$ is an algebraic integer which generates $K_{(N_k)}$ over $K$ by Lemmas 3.3(i) and 3.2(iii). Thus the element

\[\beta = g[0^{1/N_1}](\theta_K)^{12N_1} \prod_{s=2}^{t} g[0^{1/N_s}](\theta_K)^{12N_s}(K_{(N_s)}, K_{(N_{s-1})})
\]

satisfies

\[K_{(N_k)} = K(N_{K_{(N_s)}}, K_{(N_{s-1})})(\beta^n) \quad (1 \leq k \leq t)
\]

by Theorem 4.2. Moreover, by Lemma 3.3 and (4), each denominator in the above expression of $\beta$ can be rewritten as

\[N_{K_{(N_s)}}, K_{(N_{s-1})}}(g[0^{1/N_s}](\theta_K)^{12N_s}) = \prod_{u-vBw-Cv \in W_s/(\pm I_2)} g[0^{v/N_s}](\theta_K)^{12N_s},
\]

where $\min(\theta_K , Q) = x^2 + Bx + C \in \mathbb{Z}[x]$ and

\[W_s = \left\{ \gamma = \begin{bmatrix} u-Bv & -Cv \\ v & u \end{bmatrix} \in \text{GL}_2(\mathbb{Z}/N_s\mathbb{Z}) \mid u, v \in \mathbb{Z}/N_s\mathbb{Z}, \gamma \equiv \pm I_2 \pmod{N_{s-1}} \right\}.
\]
Remark 4.4. Let \( \mathfrak{f} \) be a nontrivial integral ideal of \( K \). In 1964 Ramachandra ([11, Theorem 10]) constructed a theoretically beautiful universal generator of \( K_\mathfrak{f} \) with respect to relative norm by applying Kronecker’s limit formula. His generator, however, seems to involve overly complicated products of high powers of singular values of the Klein forms and the modular discriminant function.

5 Normal bases

Let \( U/L \) be an abelian extension of number fields with \( d = [U : L] \geq 2 \) and \( G = \text{Gal}(U/L) = \{g_1 = \text{id}, g_2, \ldots, g_d\} \). Take a nonzero algebraic integer \( \alpha \) which generates \( U \) over \( L \). For each pair of

\[
\chi \in \mathcal{G} \quad \text{and} \quad 0 \leq m \leq d - 1,
\]

we let

\[
S(\chi, m) = \sum_{k=1}^{d} \chi(g_k^{-1}) \alpha_k^m \quad \text{with} \quad \alpha_k = \alpha g_k.
\]

Then it is an algebraic integer in \( U(\zeta_d) \).

Lemma 5.1. For a given character \( \chi \in \mathcal{G} \), at least one of

\[
S(\chi, 0), S(\chi, 1), \ldots, S(\chi, d - 1)
\]

is nonzero.

Proof. On the contrary, assume that

\[
S(\chi, 0) = S(\chi, 1) = \cdots = S(\chi, d - 1) = 0.
\]

Then, we derive that

\[
\begin{bmatrix}
S(\chi, 0) \\
S(\chi, 1) \\
\vdots \\
S(\chi, d - 1)
\end{bmatrix} = \begin{bmatrix}
\sum_{k=1}^{d} \chi(g_k^{-1}) \alpha_k^0 \\
\sum_{k=1}^{d} \chi(g_k^{-1}) \alpha_k^1 \\
\vdots \\
\sum_{k=1}^{d} \chi(g_k^{-1}) \alpha_k^{d-1}
\end{bmatrix} = \begin{bmatrix}
\alpha_1^0 & \alpha_2^0 & \cdots & \alpha_d^0 \\
\alpha_1^1 & \alpha_2^1 & \cdots & \alpha_d^1 \\
\vdots & \vdots & \ddots & \vdots \\
\alpha_1^{d-1} & \alpha_2^{d-1} & \cdots & \alpha_d^{d-1}
\end{bmatrix} \begin{bmatrix}
\chi(g_1^{-1}) \\
\chi(g_2^{-1}) \\
\vdots \\
\chi(g_d^{-1})
\end{bmatrix} = \begin{bmatrix}
0 \\
0 \\
\vdots \\
0
\end{bmatrix}.
\]

Now that

\[
\begin{vmatrix}
\alpha_1^0 & \alpha_2^0 & \cdots & \alpha_d^0 \\
\alpha_1^1 & \alpha_2^1 & \cdots & \alpha_d^1 \\
\vdots & \vdots & \ddots & \vdots \\
\alpha_1^{d-1} & \alpha_2^{d-1} & \cdots & \alpha_d^{d-1}
\end{vmatrix} = \prod_{1 \leq i < j \leq d} (\alpha_j - \alpha_i) \neq 0
\]
by the Vandermonde determinant formula, we attain
\[
\begin{bmatrix}
\chi(g_1^{-1}) \\
\chi(g_2^{-1}) \\
\vdots \\
\chi(g_d^{-1})
\end{bmatrix}
= \begin{bmatrix}
0 \\
0 \\
\vdots \\
0
\end{bmatrix},
\]
which is impossible. Therefore, at least one of
\[S(\chi, 0), S(\chi, 1), \ldots, S(\chi, d - 1)\]
must be nonzero as desired.

Let
\[\hat{G} = \{\chi_1, \chi_2, \ldots, \chi_d\}.\]
For each pair of
\[\chi_i \in \hat{G} \quad \text{and} \quad 0 \leq m \leq d - 1,\]
let
\[N(\chi_i, m) = |N_{U(\zeta_d)/\mathbb{Q}}(S(\chi_i, m))|.\]
For a sequence of these \(d^2\) nonnegative integer
\[N(\chi_1, 0), \quad N(\chi_2, 0), \quad \ldots, \quad N(\chi_d, 0),\]
\[N(\chi_1, 1), \quad N(\chi_2, 1), \quad \ldots, \quad N(\chi_d, 1),\]
\[\ldots, \quad \ldots, \quad \ldots, \quad \ldots, \]
\[N(\chi_1, d - 1), \quad N(\chi_2, d - 1), \quad \ldots, \quad N(\chi_d, d - 1),\]
take a sequence of \(d^2\) positive integers
\[M(\chi_1, 0), \quad M(\chi_2, 0), \quad \ldots, \quad M(\chi_d, d - 1)\]
as in the proof of Lemma 2.1. Here we observe that if \(S(\chi_i, m) \neq 0\), then \(M(\chi_i, m) \geq 2\) by the property (i) in Lemma 2.1.

**Lemma 5.2.** An element \(u \in U\) is a normal element for \(U/L\) if and only if
\[\sum_{k=1}^{d} \chi(g_k^{-1})u^{g_k} \neq 0 \quad \text{for all} \quad \chi \in \hat{G}.\]

**Proof.** See [3, Proposition 2.3].
Theorem 5.3. The element
\[ \beta = \sum_{m=0}^{d-1} \left( \sum_{i=1}^{d} \frac{1}{M(\chi_i, m)} \right) \alpha^m \]
is a normal element for \( U/L \).

Proof. Let \( \chi \in \hat{G} \). By Lemma 5.1 we have
\[ S(\chi, t) \neq 0 \quad \text{for some integer } 0 \leq t \leq d - 1. \]

Suppose on the contrary that
\[ \sum_{k=1}^{d} \chi(g_k^{-1}) \beta g_k = 0. \]

Since
\[
0 = \sum_{k=1}^{d} \chi(g_k^{-1}) \sum_{m=0}^{d-1} \left( \sum_{i=1}^{d} \frac{1}{M(\chi_i, m)} \right) \alpha^m_k \\
= \frac{1}{M(\chi, t)} \sum_{k=1}^{d} \chi(g_k^{-1}) \alpha^t_k + \sum_{k=1}^{d} \sum_{0 \leq m \leq d-1, 1 \leq i \leq d} \frac{1}{M(\chi_i, m)} \chi(g_k^{-1}) \alpha^m_k \\
= \frac{1}{M(\chi, t)} S(\chi, t) + \sum_{k=1}^{d} \sum_{0 \leq m \leq d-1, 1 \leq i \leq d} \frac{1}{M(\chi_i, m)} \chi(g_k^{-1}) \alpha^m_k, \]
we get by multiplying \( \prod_{0 \leq m \leq d-1, 1 \leq i \leq d} M(\chi_i, m) \) that
\[ S(\chi, t) \prod_{0 \leq m \leq d-1, 1 \leq i \leq d} M(\chi_i, m) = M(\chi, t) \cdot \text{(an algebraic integer)}. \]

It then follows from the fact
\[ \gcd \left( \prod_{0 \leq m \leq d-1, 1 \leq i \leq d} M(\chi_i, m), M(\chi, t) \right) = 1 \]
that \( M(\chi, t) \geq 2 \) must divide \( S(\chi, t) \), and hence it also divides the positive integer
\[ N(\chi, t) = |N_{U(\zeta_d)/Q}(S(\chi, t))|. \]
However, the fact
\[ \gcd(M(\chi, t), N(\chi, t)) = 1 \]
gives rise to a contradiction.

Therefore, we conclude by Lemma 5.2 that \( \beta \) forms a normal basis for \( U/L \). \( \square \)
Example 5.4. Let $K$ be an imaginary quadratic field of discriminant $d_K$ other than $\mathbb{Q}(\sqrt{-1})$ and $\mathbb{Q}(\sqrt{-3})$. Let $\theta_K$ be as in [5]. For an integer $N \geq 2$, the special value $g[\sigma_{1/N}] (\theta_K)^{12N}$ generates $K(N)$ over $K$ by Lemma 3.2(iii), and is an algebraic integer by Lemma 3.4(i). One can then apply Theorem 5.3 to the case where $U = K(N)$, $L = K$, $G = \text{Gal}(K(N)/K)$, $\hat{G} = \{\chi_1, \chi_2, \ldots, \chi_d\}$ and $\alpha = g[\sigma_{1/N}] (\theta_K)^{12N}$, and hence

$$\sum_{m=0}^{d-1} \left( \sum_{i=1}^{d} \frac{1}{M(\chi_i, m)} \right) g[\sigma_{1/N}] (\theta_K)^{12Nm}$$

is a normal element for $K(N)/K$.

Remark 5.5. Jung et al. showed in [3] that $g[\sigma_{1/N}] (\theta_K)^{-12N}$ is a normal element for $K(N)/K$ for a sufficiently large positive integer $\ell$. But, they couldn’t further express $\ell$ precisely in terms of $d_K$ and $N$. In other words, they took $\ell$ so large that

$$\left| \frac{(g[\sigma_{1/N}] (\theta_K)^{-12N})^\sigma}{g[\sigma_{1/N}] (\theta_K)^{-12N}} \right| \leq \frac{1}{[K(N):K]}$$

for all $\sigma \in \text{Gal}(K(N)/K)$ with $\sigma \neq \text{id}$.

6 Integrality of weakly holomorphic modular functions

Let $N$ be a positive integer and $h \in \mathcal{F}_N$ be weakly holomorphic (that is, $h$ is holomorphic on $\mathbb{H}$). As we have seen in §3, Examples 4.3 and 5.4, the integrality of special values of $h$ plays an important role of finding concrete and nontrivial examples. In this section we shall show that the integrality of special values of $h$ at all imaginary quadratic arguments implies the integrality of $h$ over $\mathbb{Z}[j]$ as a function.

Lemma 6.1. 

(i) Let $f \in \mathcal{F}_1(\zeta_N)$. If it is weakly holomorphic, then it is a polynomial of $j$ over $\mathbb{Q}(\zeta_N)$.

(ii) For any imaginary quadratic argument $\theta \in \mathbb{H}$, $j(\theta)$ is an algebraic integer.

Proof. 

(i) See [8] Chapter 5, Theorem 2.

(ii) See [8] chapter 5, Theorem 4.
Let $K$ be an imaginary quadratic field of discriminant $d_K$, and let $\theta_K$ be as in (5). We denote the class number of $K$ by $h(K)$, that is, $h(K) = [H_K : K]$. Due to Siegel and Deuring we have the following lemma.

**Lemma 6.2.**

(i) $h(K) \to \infty$ as $|d_K| \to \infty$.

(ii) If $p$ is any prime factor of $|\text{disc}(j(\theta_K), H_K/K)|$, then it does not split in $K$, equivalently, $(\frac{d_k}{p}) \neq 1$.

**Proof.** (i) See [14].

(ii) See [2] or [8, §13.4].

**Remark 6.3.** Note that $j$ has integer Fourier coefficients with respect to $q = e^{2\pi i\tau}$ [8, p.45]. So, $j(\theta_K)$ is a real algebraic integer by the definition (5) and Lemma 6.1(ii), and hence $\min(j(\theta_K), K)$ has integer coefficients.

**Lemma 6.4.** Let $m$ and $N$ be positive integers, and consider a function

\[
\begin{align*}
g(\tau) &= c_mj(\tau)^m + \cdots + c_1j(\tau) + c_0 \in \mathbb{Q}(\zeta_N)[j(\tau)].
\end{align*}
\]

Assume that $g(\theta)$ is an algebraic integer for every imaginary quadratic argument $\theta \in \mathbb{H}$. Then $g(\tau)$ belongs to $\mathbb{Z}[\zeta_N][j(\tau)]$.

**Proof.** We can take a sufficiently large prime $t$ such that $-t \equiv 1 \pmod{4}$ and $h(K) \geq m + 1$, when $K = \mathbb{Q}(\sqrt{-t})$, by the Dirichlet theorem and Lemma 6.2(i). Let

\[
j(\theta_1), j(\theta_2), \ldots, j(\theta_{h(K)})
\]

be Galois conjugates of $j(\theta_K)$ over $K$ (here, $\theta_K$ is an element of $\mathbb{H}$ depending on $K$ as given in (5)), where $\theta_k \in \mathbb{H}$ ($k = 1, 2, \ldots, h(K)$) give rise to ideal class representatives $[\theta_k, 1]$ of $K$. Setting $\tau = \theta_k$ ($k = 1, 2, \ldots, m + 1$) in (12) we get a linear system (in unknowns $c_0, c_1, \ldots, c_m$)

\[
\begin{bmatrix}
1 & j(\theta_1) & \cdots & j(\theta_1)^m \\
1 & j(\theta_2) & \cdots & j(\theta_2)^m \\
\vdots & \vdots & \ddots & \vdots \\
1 & j(\theta_{m+1}) & \cdots & j(\theta_{m+1})^m
\end{bmatrix}
\begin{bmatrix}
c_0 \\
c_1 \\
\vdots \\
c_m
\end{bmatrix}
= \begin{bmatrix}
g(\theta_1) \\
g(\theta_2) \\
\vdots \\
g(\theta_{m+1})
\end{bmatrix}.
\]

Observe that all entries of the augmented matrix of the linear system are algebraic integers by Lemma 6.1(ii) and the hypothesis. Furthermore, since the determinant of the coefficient matrix is given by

\[
\prod_{1 \leq \ell < k \leq m+1} (j(\theta_k) - j(\theta_{\ell}))
\]
by the Vandermonde determinant formula, we deduce that

\[(13) \quad c_0, c_1, \ldots, c_m \in \frac{1}{D} \mathbb{Z}[\zeta_N], \quad \text{where} \quad D = |\text{disc}(j(\theta_K), H_K/K)|.\]

Let \(s_1, s_2, \ldots, s_\nu\) be all prime factors of \(D\). Then one can also take a suitably large prime \(v\) such that \(-v \equiv 1 \pmod{4}\) and \(-v \equiv 1 \pmod{s_k}\) for all \(k = 1, 2, \ldots, \nu\), and \(h(L) \geq m + 1\) with \(L = \mathbb{Q}(\sqrt{-v})\). In exactly the same way as above we achieve that

\[(14) \quad c_0, c_1, \ldots, c_m \in \frac{1}{M} \mathbb{Z}[\zeta_N], \quad \text{where} \quad M = |\text{disc}(j(\theta_L), H_L/L)|.\]

Now, let \(p\) be a prime factor of \(D\) so that \(p = s_k\) for some index \(1 \leq k \leq \nu\). We then obtain

\[
\left(\frac{d_L}{p}\right) = \left(\frac{-v}{s_k}\right) = \left(\frac{1}{s_k}\right) = 1,
\]

because \(-v \equiv 1 \pmod{4}\) and \(-v \equiv 1 \pmod{s_k}\). Thus \(p\) does not divide \(M\) by Lemma 6.2(ii), and hence we get \(\gcd(D, M) = 1\). Considering prime ideal factorizations in \(\mathbb{Z}[\zeta_N]\), we readily deduce from (13) and (14) that \(c_0, c_1, \ldots, c_m\) lie in \(\mathbb{Z}[\zeta_N]\). Therefore, we accomplish the lemma.

**Remark 6.5.** Lemma 6.4 is obvious when \(m = 0\).

Let \(N\) be a positive integer. The field \(\mathcal{F}_N\) is a Galois extension of \(\mathcal{F}_1(\zeta_N)\) whose Galois group is isomorphic to \(\text{SL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I_2\}\). More precisely, an element \(\gamma\) in \(\text{SL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I_2\}\) acts on \(f \in \mathcal{F}_N\) by

\[
f^\gamma = f \circ \tilde{\gamma},
\]

where \(\tilde{\gamma}\) is any preimage of the reduction \(\text{SL}_2(\mathbb{Z}) \rightarrow \text{SL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I_2\}\) that acts on \(\mathbb{H}\) as fractional linear transformation (\(\mathcal{I}_3\) §6.2).

**Theorem 6.6.** Let \(h \in \mathcal{F}_N\) be weakly holomorphic. Then, \(h\) is integral over \(\mathbb{Z}[j]\) if and only if \(h(\theta)\) is an algebraic integer for any imaginary quadratic argument \(\theta \in \mathbb{H}\).

**Proof.** Assume that \(h\) is integral over \(\mathbb{Z}[j]\), so \(h\) satisfies

\[(15) \quad h^n + a_{n-1}h^{n-1} + \cdots + a_1h + a_0 = 0\]

for some \(a_k = a_k(\tau) \in \mathbb{Z}[j(\tau)] (k = 0, 1, \ldots, n-1)\). Let \(\theta \in \mathbb{H}\) be imaginary quadratic. If we set \(\tau = \theta\) in (15), then we get

\[(16) \quad h(\theta)^n + a_{n-1}(\theta)h(\theta)^{n-1} + \cdots + a_1(\theta)h(\theta) + a_0(\theta) = 0.\]

Since \(j(\theta)\) is an algebraic integer by Lemma 6.1(ii) and \(a_k(\theta) (k = 0, 1, \ldots, n-1)\) are polynomials of \(j(\theta)\) over \(\mathbb{Z}\), we see from (16) that \(h(\theta)\) is an algebraic integer, too.
Conversely, assume that $h(\theta)$ is an algebraic integer for any imaginary quadratic argument $\theta \in \mathbb{H}$. Let \( SL_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I_2\} = \{\gamma_1, \gamma_2, \ldots, \gamma_m\} \). For each $\gamma_k$, let $\tilde{\gamma}_k$ be its preimage under the reduction $SL_2(\mathbb{Z}) \to SL_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I_2\}$. Consider the polynomial

\[
p(x) = \prod_{k=1}^{m} (x - h^{\gamma_k}) = \prod_{k=1}^{m} (x - h \circ \tilde{\gamma}_k) = x^m + b_{m-1}x^{m-1} + \cdots + b_1x + b_0 \in \mathcal{F}_1(\zeta_N)[x].
\]

Since its coefficients $b_s = b_s(\tau)$ ($s = 0, 1, \ldots, m - 1$) are symmetric polynomials of $h \circ \tilde{\gamma}_k$ ($k = 1, 2, \ldots, m$) which are holomorphic on $\mathbb{H}$, they are polynomials of $j(\tau)$ over $\mathbb{Q}(\zeta_N)$ by Lemma 6.1(i). Furthermore, let $\theta \in \mathbb{H}$ be imaginary quadratic. Then, $\tilde{\gamma}_k(\theta)$ ($k = 1, 2, \ldots, m$) lie in $\mathbb{H}$ and are imaginary quadratic, too. And, it follows that $(h \circ \tilde{\gamma}_k(\theta))$ are algebraic integers by our assumption, and hence their symmetric polynomials $b_s(\theta)$ ($s = 0, 1, \ldots, m - 1$) are also algebraic integers. The result follows from Lemma 6.4.

References

[1] S. Chowla, The nonexistence of nontrivial linear relations between the roots of a certain irreducible equation, J. Number Theory 2 (1970), 120–123.

[2] M. Deuring, Teilbarkeitseigenschaften der singularen Moduln der elliptischen Funktionen und die Diskriminante der Klassengleichung, Comment. Math. Helv. 19 (1946), 74–82.

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

[4] K. Komatsu, Construction of a normal basis by special values of Siegel modular functions, Proc. Amer. Math. Soc. 128 (2000), no. 2, 315–323.

[5] J. K. Koo and D. H. Shin, On some arithmetic properties of Siegel functions, Math. Zeit. 264 (2010), no. 1, 137–177.

[6] J. K. Koo and D. H. Shin, On some theta constants and class fields, arXiv:1202.3213.

[7] D. Kubert and S. Lang, Modular Units, Grundlehren der mathematischen Wissenschaften 244, Spinger-Verlag, 1981.

[8] S. Lang, Elliptic Functions, 2nd ed., Spinger-Verlag, New York, 1987.

[9] T. Okada, On an extension of a theorem of S. Chowla, Acta Arith. 38 (1980/81), no. 4, 341–345.
[10] T. Okada, *Normal bases of class field over Gauss’ number field*, J. London Math. Soc. (2) 22 (1980), no. 2, 221–225.

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

[12] R. Schertz, *Galoismodulstruktur und elliptische Funktionen*, J. Number Theory. 39 (1991), no. 3, 285–326.

[13] G. Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions*, Iwanami Shoten and Princeton University Press, Princeton, N. J., 1971.

[14] C. L. Siegel, *Über die Classenzahl quadratischer Zahlkörper*, Acta Arith. 1 (1935), 83–86.

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

[16] M. J. Talyor, *Relative Galois module structure of rings of integers and elliptic functions II*, Ann. of Math. (2) 121 (1985), no. 3, 519–535.

[17] B. L. van der Waerden, *Algebra, Vol I*, Springer-Verlag, 2003.