Bull. Aust. Math. Soc. **95** (2017), 384–392
doi:10.1017/S0004972716001362

NORMAL BASES FOR MODULAR FUNCTION FIELDS

JA KYUNG KOO, DONG HWA SHIN and DONG SUNG YOON✉

(Received 9 August 2016; accepted 25 November 2016; first published online 2 March 2017)

Abstract

We provide a concrete example of a normal basis for a finite Galois extension which is not abelian. More precisely, let $\mathbb{C}(X(N))$ be the field of meromorphic functions on the modular curve $X(N)$ of level N. We construct a completely free element in the extension $\mathbb{C}(X(N))/\mathbb{C}(X(1))$ by means of Siegel functions.

2010 *Mathematics subject classification*: primary 11F03; secondary 11G16.

Keywords and phrases: modular functions, modular units, normal bases.

1. Introduction

Let E be a finite Galois extension of a field F with

$$G = \mathrm{Gal}(E/F) = \{\sigma_1, \sigma_2, \ldots, \sigma_n\}.$$

The well-known normal basis theorem (see [12]) states that there always exists an element a of E for which

$$\{a^{\sigma_1}, a^{\sigma_2}, \ldots, a^{\sigma_n}\}$$

is a basis for E over F. We call such a basis a *normal basis* for the extension E/F and say that the element a is *free* in E/F. In other words, E is a free $F[G]$-module of rank one generated by a. Blessenohl and Johnson proved in [1] that there is a primitive element a for E/F which is free in E/L for every intermediate field L of E/F. Such an element a is said to be *completely free* in the extension E/F. Not much is known about explicit constructions of (completely) free elements when F is infinite. When F is a number field, we refer to [2, 7–9, 11]. In [4], there is an example of completely free elements in function field extensions which are abelian.

For a positive integer N, let

$$\Gamma(N) = \{\sigma \in \mathrm{SL}_2(\mathbb{Z}) \mid \sigma \equiv I_2 \ (\mathrm{mod}\ N \cdot M_2(\mathbb{Z}))\}$$

The second author was supported by Hankuk University of Foreign Studies Research Fund of 2016.

be the principal congruence subgroup of $SL_2(\mathbb{Z})$ of level N which acts on the upper half-plane $\mathbb{H} = \{\tau \in \mathbb{C} \mid \mathrm{Im}(\tau) > 0\}$ by fractional linear transformations. Corresponding to $\Gamma(N)$, let

$$X(N) = \Gamma(N)\backslash\mathbb{H}^*$$

be the modular curve of level N, where $\mathbb{H}^* = \mathbb{H} \cup \mathbb{Q} \cup \{i\infty\}$ [10, Ch. 1]. We denote its meromorphic function field by $\mathbb{C}(X(N))$. As is well known, $\mathbb{C}(X(N))$ is a Galois extension of $\mathbb{C}(X(1))$ with

$$\mathrm{Gal}(\mathbb{C}(X(N))/\mathbb{C}(X(1))) \simeq \Gamma(1)/\pm\Gamma(N) \simeq SL_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I_2\} \tag{1.1}$$

([6, Ch. 6, Theorem 2] and [10, Proposition 6.1]). Further, if $N \geq 2$, then $\mathbb{C}(X(N))$ is not an abelian extension of $\mathbb{C}(X(1))$. We shall find a completely free element $g(\tau)$ in $\mathbb{C}(X(N))/\mathbb{C}(X(1))$ in terms of Siegel functions (Theorem 3.3). This gives a concrete example of a normal basis for a nonabelian Galois extension.

Let K be an imaginary quadratic field and let $K_{(N)}$ be the ray class field of K modulo N for an integer $N \geq 2$. Jung *et al.* showed in [3] that a certain function in $\mathbb{C}(X(N))$ evaluated at a point in K becomes a completely free element in $K_{(N)}/K$. We conjecture that the completely free element in the function field extension $\mathbb{C}(X(N))/\mathbb{C}(X(1))$ given in Theorem 3.3 will also give rise to a completely free element in the number field extension $K_{(N)}/K$.

2. Siegel functions as modular functions

We briefly introduce Siegel functions and their basic properties and develop some results for later use.

For a lattice Λ in $\mathbb{C}$, the *Weierstrass σ-function* relative to Λ is defined by

$$\sigma(z;\Lambda) = z\prod_{\lambda\in\Lambda\backslash\{0\}}\Big(1-\frac{z}{\lambda}\Big)\exp\Big(\frac{z}{\lambda}+\frac{z^2}{2\lambda^2}\Big), \quad z \in \mathbb{C}.$$

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

$$\zeta(z;\Lambda) = \frac{\sigma'(z;\Lambda)}{\sigma(z;\Lambda)} = \frac{1}{z} + \sum_{\lambda\in\Lambda\backslash\{0\}}\Big(\frac{1}{z-\lambda}+\frac{1}{\lambda}+\frac{z}{\lambda^2}\Big), \quad z \in \mathbb{C}.$$

One can readily see that

$$\zeta'(z;\Lambda) = -\frac{1}{z^2} + \sum_{\lambda\in\Lambda\backslash\{0\}}\Big(-\frac{1}{(z-\lambda)^2}+\frac{1}{\lambda^2}\Big),$$

which is periodic with respect to Λ. Thus, for each $\lambda \in \Lambda$, there is a constant $\eta(\lambda;\Lambda)$ such that

$$\zeta(z+\lambda;\Lambda) - \zeta(z;\Lambda) = \eta(\lambda;\Lambda), \quad z \in \mathbb{C}.$$

https://doi.org/10.1017/S0004972716001362 Published online by Cambridge University Press

Now, for $\mathbf{v} = \left[\begin{smallmatrix} v_1 \\ v_2 \end{smallmatrix}\right] \in \mathbb{Q}^2 \setminus \mathbb{Z}^2$, we define the *Siegel function* $g_{\mathbf{v}}(\tau)$ for $\tau \in \mathbb{H}$ by

$$g_{\mathbf{v}}(\tau) = \exp(-(1/2)(v_1\eta(\tau;[\tau,1]) + v_2\eta(1;[\tau,1]))(v_1\tau + v_2))\sigma(v_1\tau + v_2;[\tau,1])\eta(\tau)^2,$$

where $[\tau, 1] = \tau\mathbb{Z} + \mathbb{Z}$ and $\eta(\tau)$ is the *Dedekind η-function* given by

$$\eta(\tau) = \sqrt{2\pi} e^{\pi i/4} q^{1/24} \prod_{n=1}^{\infty} (1 - q^n), \quad q = e^{2\pi i\tau}, \tau \in \mathbb{H}.$$

Let

$$\mathbf{B}_2(x) = x^2 - x + \tfrac{1}{6}, \quad x \in \mathbb{R}$$

be the second Bernoulli polynomial and let $\langle x \rangle$ be the fractional part of x in the interval $[0, 1)$.

Proposition 2.1. *Let* $\mathbf{v} = \left[\begin{smallmatrix} v_1 \\ v_2 \end{smallmatrix}\right] \in (1/N)\mathbb{Z}^2 \setminus \mathbb{Z}^2$ *for an integer* $N \geq 2$.

(i) [5, K 4 on page 29] $g_{\mathbf{v}}(\tau)$ *has the infinite product expansion*

$$g_{\mathbf{v}}(\tau) = -e^{\pi i v_2(v_1-1)} q^{(1/2)\mathbf{B}_2(v_1)} (1 - q^{v_1} e^{2\pi i v_2}) \prod_{n=1}^{\infty} (1 - q^{n+v_1} e^{2\pi i v_2})(1 - q^{n-v_1} e^{-2\pi i v_2})$$

with respect to $q = e^{2\pi i\tau}$.

(ii) [5, page 31] *The q-order of* $g_{\mathbf{v}}(\tau)$ *is given by*

$$\mathrm{ord}_q g_{\mathbf{v}}(\tau) = \tfrac{1}{2}\mathbf{B}_2(\langle v_1 \rangle).$$

(iii) [5, Ch. 2, Theorem 1.2] $g_{\mathbf{v}}(\tau)^{12N}$ *belongs to* $\mathbb{C}(X(N))$ *and has neither zeros nor poles on* $\mathbb{H}$.

(iv) [5, Ch. 2, Proposition 1.3] $g_{\mathbf{v}}(\tau)^{12N}$ *depends only on* $\pm\mathbf{v}$ $(\mathrm{mod}\ \mathbb{Z}^2)$ *and satisfies*

$$(g_{\mathbf{v}}(\tau)^{12N})^{\sigma} = (g_{\mathbf{v}}^{12N} \circ \sigma)(\tau) = g_{\sigma^T\mathbf{v}}(\tau)^{12N}, \quad \sigma \in \mathrm{SL}_2(\mathbb{Z}),$$

where σ^T *stands for the transpose of* σ.

For a positive integer N, let $\Gamma_1(N)$ be the congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$ defined by

$$\Gamma_1(N) = \left\{ \sigma \in \mathrm{SL}_2(\mathbb{Z}) \;\middle|\; \sigma \equiv \begin{bmatrix} 1 & * \\ 0 & 1 \end{bmatrix} \ (\mathrm{mod}\ N \cdot M_2(\mathbb{Z})) \right\}.$$

Now we let $N \geq 2$ and consider the function

$$g(\tau) = g_{\left[\begin{smallmatrix} 0 \\ 1/N \end{smallmatrix}\right]}(\tau)^{-12N\ell} g_{\left[\begin{smallmatrix} 1/N \\ 0 \end{smallmatrix}\right]}(\tau)^{-12Nm},$$

where ℓ and m are integers such that $\ell > m > 0$. From Proposition 2.1(iii), $g(\tau)$ belongs to $\mathbb{C}(X(N))$.

https://doi.org/10.1017/S0004972716001362 Published online by Cambridge University Press

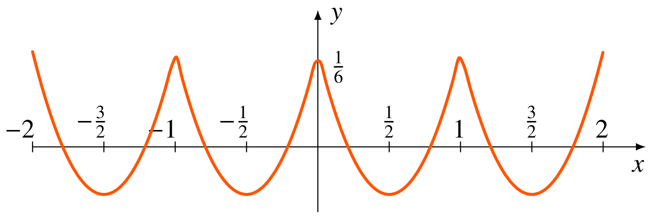

FIGURE 1. The graph of $y = \mathbf{B}_2(\langle x \rangle)$.

LEMMA 2.2. *For all $\sigma \in \mathrm{SL}_2(\mathbb{Z})$,*

$$\mathrm{ord}_q\left(\frac{g(\tau)^\sigma}{g(\tau)}\right) \geq 0.$$

The equality holds if and only if $\sigma \in \pm\Gamma_1(N)$.

PROOF. Let $\sigma = \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \in \mathrm{SL}_2(\mathbb{Z})$. Note that $a \equiv c \equiv 0 \pmod N$ is impossible. We get by Proposition 2.1(iv) and (ii) that

$$\begin{aligned}\mathrm{ord}_q\left(\frac{g(\tau)^\sigma}{g(\tau)}\right) &= \mathrm{ord}_q\left(\frac{g_{\left[\begin{smallmatrix} c/N \\ d/N \end{smallmatrix}\right]}(\tau)^{-12N\ell} g_{\left[\begin{smallmatrix} a/N \\ b/N \end{smallmatrix}\right]}(\tau)^{-12Nm}}{g_{\left[\begin{smallmatrix} 0 \\ 1/N \end{smallmatrix}\right]}(\tau)^{-12N\ell} g_{\left[\begin{smallmatrix} 1/N \\ 0 \end{smallmatrix}\right]}(\tau)^{-12Nm}}\right) \\ &= 6N(\ell\mathbf{B}_2(0) + m\mathbf{B}_2(1/N) - \ell\mathbf{B}_2(\langle c/N \rangle) - m\mathbf{B}_2(\langle a/N \rangle)).\end{aligned}$$

From the fact that $\ell > m > 0$ and Figure 1, we deduce that

$$\mathrm{ord}_q\left(\frac{g(\tau)^\sigma}{g(\tau)}\right) \geq 0$$

with equality if and only if

$$\langle c/N \rangle = 0 \quad \text{and} \quad \langle a/N \rangle = 1/N \text{ or } 1 - 1/N. \tag{2.1}$$

Moreover, by the relation $\det(\sigma) = ad - bc = 1$, the condition (2.1) amounts to

$$\sigma \equiv \pm \begin{bmatrix} 1 & * \\ 0 & 1 \end{bmatrix} \pmod{N \cdot M_2(\mathbb{Z})}.$$

This proves the lemma. □

Let $\mathbb{R}_+$ denote the set of positive real numbers.

LEMMA 2.3. *Given any $\varepsilon \in \mathbb{R}_+$, we can take $r \in \mathbb{R}_+$ and an integer m large enough so that*

$$\left|\frac{g^\sigma(ri)}{g(ri)}\right| < \varepsilon \quad \textit{for all } \sigma \in \mathrm{SL}_2(\mathbb{Z}) \setminus \pm\Gamma(N).$$

https://doi.org/10.1017/S0004972716001362 Published online by Cambridge University Press

Proof. First, consider the case where $\sigma \notin \pm\Gamma_1(N)$. By Lemma 2.2,

$$\mathrm{ord}_q\Big(\frac{g(\tau)^\sigma}{g(\tau)}\Big) > 0,$$

which implies that $g(\tau)^\sigma/g(\tau)$ has a zero at the cusp $i\infty$. Hence we can take $r_\sigma \in \mathbb{R}_+$ sufficiently large so that

$$\left|\frac{g^\sigma(r_\sigma i)}{g(r_\sigma i)}\right| < \varepsilon.$$

Set

$$r = \max\{r_\sigma \mid \sigma \in \mathrm{SL}_2(\mathbb{Z})\backslash \pm\Gamma_1(N)\}.$$

Second, let $\sigma \in \pm\Gamma_1(N)\backslash \pm\Gamma(N)$, so that $\sigma \equiv \pm\left[\begin{smallmatrix}1 & b\\ 0 & 1\end{smallmatrix}\right] \pmod{N \cdot M_2(\mathbb{Z})}$ for some $b \in \mathbb{Z}$ with $b \not\equiv 0 \pmod N$. Then

$$\begin{aligned}
\left|\frac{g^\sigma(ri)}{g(ri)}\right| &= \left|\frac{g_{\left[\begin{smallmatrix}0\\1/N\end{smallmatrix}\right]}(ri)^{-12N\ell} g_{\left[\begin{smallmatrix}1/N\\b/N\end{smallmatrix}\right]}(ri)^{-12Nm}}{g_{\left[\begin{smallmatrix}0\\1/N\end{smallmatrix}\right]}(ri)^{-12N\ell} g_{\left[\begin{smallmatrix}1/N\\0\end{smallmatrix}\right]}(ri)^{-12Nm}}\right| \quad \text{(by Proposition 2.1(iv))}\\
&= \left|\frac{g_{\left[\begin{smallmatrix}1/N\\0\end{smallmatrix}\right]}(ri)}{g_{\left[\begin{smallmatrix}1/N\\b/N\end{smallmatrix}\right]}(ri)}\right|^{12Nm}\\
&= \left|\frac{1-R^{1/N}}{1-R^{1/N}\zeta_N^b}\right|^{12Nm} \prod_{n=1}^{\infty}\left|\frac{(1-R^{n+1/N})(1-R^{n-1/N})}{(1-R^{n+1/N}\zeta_N^b)(1-R^{n-u}\zeta_N^{-b})}\right|^{12Nm}\\
&\qquad \text{(by Proposition 2.1(i), where } R = e^{-2\pi r} \text{ and } \zeta_N = e^{2\pi i/N})\\
&\le \left|\frac{1-R^{1/N}}{1-R^{1/N}\zeta_N^b}\right|^{12Nm}
\end{aligned}$$

because $|1-x| \le |1-x\zeta|$ for any $x \in \mathbb{R}_+$ with $x < 1$ and any root of unity ζ. Therefore, if m is sufficiently large,

$$\left|\frac{g^\sigma(ri)}{g(ri)}\right| < \varepsilon.$$

This completes the proof. □

3. Completely free elements in modular function fields

Let $N \ge 2$. In this section, we shall show that the elements

$$g(\tau) = g_{\left[\begin{smallmatrix}0\\1/N\end{smallmatrix}\right]}(\tau)^{-12N\ell} g_{\left[\begin{smallmatrix}1/N\\0\end{smallmatrix}\right]}(\tau)^{-12Nm} \quad \text{with } \ell > m > 0$$

play an important role as completely normal elements in modular function field extensions.

https://doi.org/10.1017/S0004972716001362 Published online by Cambridge University Press

Proposition 3.1. *The function $g(\tau)$ generates $\mathbb{C}(X(N))$ over $\mathbb{C}(X(1))$.*

Proof. Suppose that $\sigma = \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \in \mathrm{SL}_2(\mathbb{Z})$ leaves $g(\tau)$ fixed. In particular, since $\mathrm{ord}_q g(\tau) = \mathrm{ord}_q g(\tau)^\sigma$, Lemma 2.2 implies that $\sigma \in \pm\Gamma_1(N)$. Furthermore, by Proposition 2.1(iv) and (ii),

$$\begin{aligned}
\mathrm{ord}_q g(\tau)^{\left[\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right]} &= \mathrm{ord}_q\Big(g_{\left[\begin{smallmatrix} 1/N \\ 0 \end{smallmatrix}\right]}(\tau)^{-12N\ell} g_{\left[\begin{smallmatrix} 0 \\ -1/N \end{smallmatrix}\right]}(\tau)^{-12Nm}\Big) \\
&= -6N\ell\mathbf{B}_2(1/N) - 6Nm\mathbf{B}_2(0) \\
&= \mathrm{ord}_q(g(\tau)^\sigma)^{\left[\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right]} \\
&= \mathrm{ord}_q g(\tau)^{\left[\begin{smallmatrix} b & -a \\ d & -c \end{smallmatrix}\right]} \\
&= \mathrm{ord}_q\Big(g_{\left[\begin{smallmatrix} d/N \\ -c/N \end{smallmatrix}\right]}(\tau)^{-12N\ell} g_{\left[\begin{smallmatrix} b/N \\ -a/N \end{smallmatrix}\right]}(\tau)^{-12Nm}\Big) \\
&= -6N\ell\mathbf{B}_2(\langle d/N\rangle) - 6Nm\mathbf{B}_2(\langle b/N\rangle).
\end{aligned}$$

Thus we obtain $b \equiv 0 \pmod N$ and hence $\sigma \in \pm\Gamma(N)$. Therefore, we conclude by (1.1) and the Galois theory that $g(\tau)$ generates $\mathbb{C}(X(N))$ over $\mathbf{C}(X(1))$. □

Theorem 3.2. *Let $X^0(N)$ be the modular curve for the congruence subgroup*

$$\Gamma^0(N) = \left\{\sigma \in \mathrm{SL}_2(\mathbb{Z}) \;\middle|\; \sigma \equiv \begin{bmatrix} * & 0 \\ * & * \end{bmatrix} \pmod{N \cdot M_2(\mathbb{Z})}\right\}$$

with the meromorphic function field $\mathbb{C}(X^0(N))$. Then the element $g(\tau)$ is completely free in $\mathbb{C}(X(N))/\mathbb{C}(X^0(N))$.

Proof. Note that $\mathbb{C}(X(N))$ is a Galois extension of $\mathbb{C}(X^0(N))$ with

$$\mathrm{Gal}(\mathbb{C}(X(N))/\mathbb{C}(X^0(N))) \simeq \Gamma^0(N)/\pm\Gamma(N).$$

From Proposition 3.1, $g(\tau)$ generates $\mathbb{C}(X(N))$ over $\mathbb{C}(X^0(N))$.

Now, let L be any intermediate field of $\mathbb{C}(X(N))/\mathbb{C}(X^0(N))$ with

$$\mathrm{Gal}(\mathbb{C}(X(N))/L) = \{\sigma_1 = \mathrm{Id}, \sigma_2, \ldots, \sigma_k\}.$$

Since $\Gamma^0(N) \cap \pm\Gamma_1(N) = \pm\Gamma(N)$,

$$\sigma_i \notin \pm\Gamma_1(N), \quad i = 2, \ldots, k. \tag{3.1}$$

Set

$$g_i = g(\tau)^{\sigma_i}, \quad i = 1, 2, \ldots, k$$

and suppose that

$$c_1 g_1 + c_2 g_2 + \cdots + c_k g_k = 0 \quad \text{for some } c_1, c_2, \ldots, c_k \in L. \tag{3.2}$$

https://doi.org/10.1017/S0004972716001362 Published online by Cambridge University Press

Let σ_i $(i = 1, 2, \ldots, k)$ act on both sides of (3.2). This yields the system of equations

$$\begin{cases} c_1 g_1^{\sigma_1} + c_2 g_2^{\sigma_1} + \cdots + c_k g_k^{\sigma_1} = 0, \\ c_1 g_1^{\sigma_2} + c_2 g_2^{\sigma_2} + \cdots + c_k g_k^{\sigma_2} = 0, \\ \qquad\qquad \vdots \\ c_1 g_1^{\sigma_k} + c_2 g_2^{\sigma_k} + \cdots + c_k g_k^{\sigma_k} = 0, \end{cases}$$

which can be rewritten as

$$A \begin{bmatrix} c_1 \\ c_2 \\ \vdots \\ c_k \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix} \quad \text{with } A = [g_j^{\sigma_i}]_{1 \le i, j \le k}.$$

Let S_k be the permutation group on $\{1, 2, \ldots, k\}$. Then

$$\begin{aligned} \det(A) &= \sum_{j_1 j_2 \cdots j_k \in S_k} \operatorname{sgn}(j_1 j_2 \cdots j_k) g_{j_1}^{\sigma_1} g_{j_2}^{\sigma_2} \cdots g_{j_k}^{\sigma_k} \\ &= \pm g^k + \sum_{\substack{j_1 j_2 \cdots j_k \in S_k \text{ such that} \\ \sigma_{j_1}\sigma_{j_2}\cdots\sigma_{j_k} \neq \sigma_1^{-1}\sigma_2^{-1}\cdots\sigma_k^{-1}}} \pm g^{\sigma_{j_1}\sigma_1} g^{\sigma_{j_2}\sigma_2} \cdots g^{\sigma_{j_k}\sigma_k} \\ &= \pm g^k \Bigg(1 + \sum_{\substack{j_1 j_2 \cdots j_k \in S_k \text{ such that} \\ \sigma_{j_1}\sigma_{j_2}\cdots\sigma_{j_k} \neq \sigma_1^{-1}\sigma_2^{-1}\cdots\sigma_k^{-1}}} \pm \Big(\frac{g^{\sigma_{j_1}\sigma_1}}{g}\Big)\Big(\frac{g^{\sigma_{j_2}\sigma_2}}{g}\Big) \cdots \Big(\frac{g^{\sigma_{j_k}\sigma_k}}{g}\Big)\Bigg). \end{aligned}$$

For each $j_1 j_2 \cdots j_k \in S_k$ with $\sigma_{j_1}\sigma_{j_2} \cdots \sigma_{j_k} \neq \sigma_1^{-1}\sigma_2^{-1} \cdots \sigma_k^{-1}$,

$$\sigma_{j_i}\sigma_i \neq \mathrm{Id} \quad \text{for some } 1 \le i \le k.$$

Thus

$$\begin{aligned} \operatorname{ord}_q \det(A) &= \operatorname{ord}_q g^k \quad \text{(by (3.1) and Lemma 2.2)} \\ &= -6kN(\ell \mathbf{B}_2(0) + m\mathbf{B}_2(1/N)) \quad \text{(by Proposition 2.1(ii))} \\ &< 0, \end{aligned}$$

from the fact that $\ell > m > 0$ and Figure 1. This implies that

$$\det(A) \neq 0 \quad \text{and} \quad c_1 = c_2 = \cdots = c_k = 0.$$

Therefore $\{g_1, g_2, \ldots, g_k\}$ is linearly independent over L and $g(\tau)$ is completely free in $\mathbb{C}(X(N))/\mathbb{C}(X^0(N))$. □

THEOREM 3.3. *There is a positive integer M for which*

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

is completely free in $\mathbb{C}(X(N))/\mathbb{C}(X(1))$ for $\ell > m > M$.

https://doi.org/10.1017/S0004972716001362 Published online by Cambridge University Press

PROOF. Let $d = [\mathbb{C}(X(N)) : \mathbb{C}(X(1))]$. From Lemma 2.3 and (1.1), there exist a positive integer M and $r \in \mathbb{R}_+$ so that, if $\ell > m > M$, then

$$\left|\frac{g^{\sigma}(ri)}{g(ri)}\right| < \frac{1}{d! - 1} \quad \text{for all } \sigma \in \mathrm{Gal}(\mathbb{C}(X(N))/\mathbb{C}(X(1))) \text{ with } \sigma \neq \mathrm{Id}. \tag{3.3}$$

Now let $\ell > m > M$. Let L be any intermediate field of $\mathbb{C}(X(N))/\mathbb{C}(X(1))$ with

$$\mathrm{Gal}(\mathbb{C}(X(N))/L) = \{\sigma_1 = \mathrm{Id}, \sigma_2, \ldots, \sigma_n\}.$$

From Proposition 3.1, $g(\tau)$ generates $\mathbb{C}(X(N))$ over L. Consider the $n \times n$ matrix

$$B = [g_j^{\sigma_i}]_{1 \le i,j \le n} \quad \text{where } g_j = g(\tau)^{\sigma_j}.$$

As in Theorem 3.2, it suffices to show that $\det(B) \neq 0$ in order to prove that $\{g_1, g_2, \ldots, g_n\}$ is linearly independent over L. We derive

$$\begin{aligned}
|\det(B)(ri)| &= \left|\sum_{j_1 j_2 \cdots j_n \in S_n} \mathrm{sgn}(j_1 j_2 \cdots j_n) g_{j_1}^{\sigma_1}(ri) g_{j_2}^{\sigma_2}(ri) \cdots g_{j_n}^{\sigma_n}(ri)\right| \\
&= \left|\pm g(ri)^n + \sum_{\substack{j_1 j_2 \cdots j_n \in S_n \text{ such that} \\ \sigma_{j_1}\sigma_{j_2}\cdots\sigma_{j_n} \neq \sigma_1^{-1}\sigma_2^{-1}\cdots\sigma_n^{-1}}} \pm g^{\sigma_{j_1}\sigma_1}(ri) g^{\sigma_{j_2}\sigma_2}(ri) \cdots g^{\sigma_{j_n}\sigma_n}(ri)\right| \\
&\ge |g(ri)|^n \left(1 - \sum_{\substack{j_1 j_2 \cdots j_n \in S_n \text{ such that} \\ \sigma_{j_1}\sigma_{j_2}\cdots\sigma_{j_n} \neq \sigma_1^{-1}\sigma_2^{-1}\cdots\sigma_n^{-1}}} \left|\frac{g^{\sigma_{j_1}\sigma_1}(ri)}{g(ri)}\right| \left|\frac{g^{\sigma_{j_2}\sigma_2}(ri)}{g(ri)}\right| \cdots \left|\frac{g^{\sigma_{j_n}\sigma_n}(ri)}{g(ri)}\right|\right) \\
&\ge |g(ri)|^n \left(1 - \sum_{\substack{j_1 j_2 \cdots j_n \in S_n \text{ such that} \\ \sigma_{j_1}\sigma_{j_2}\cdots\sigma_{j_n} \neq \sigma_1^{-1}\sigma_2^{-1}\cdots\sigma_n^{-1}}} \frac{1}{d! - 1}\right) \\
&\qquad (\text{by the fact } \sigma_{j_i}\sigma_i \neq \mathrm{Id} \text{ for some } 1 \le i \le n \text{ and } (3.3)) \\
&> |g(ri)|^n \left(1 - \frac{n! - 1}{d! - 1}\right) \\
&\ge 0.
\end{aligned}$$

Thus $\det(B) \neq 0$ and $g(\tau)$ is completely free in $\mathbb{C}(X(N))/\mathbb{C}(X(1))$, as desired. □

References

[1] D. Blessenohl and K. Johnsen, 'Eine Verschärfung des Satzes von der Normalbasis', *J. Algebra* **103**(1) (1986), 141–159.

[2] D. Hachenberger, 'Universal normal bases for the abelian closure of the field of rational numbers', *Acta Arith.* **93**(4) (2000), 329–341.

[3] H. Y. Jung, J. K. Koo and D. H. Shin, 'Normal bases of ray class fields over imaginary quadratic fields', *Math. Z.* **271**(1–2) (2012), 109–116.

[4] J. K. Koo and D. H. Shin, 'Completely normal elements in some finite abelian extensions', *Cent. Eur. J. Math.* **11**(10) (2013), 1725–1731.

[5] D. Kubert and S. Lang, *Modular Units*, Grundlehren der Mathematischen Wissenschaften, 244 (Springer, New York, 1981).

[6] S. Lang, *Elliptic Functions*, 2nd edn, Graduate Texts in Mathematics, 112 (Springer, New York, 1987).
[7] H.-W. Leopoldt, 'Über die Hauptordnung der ganzen Elemente eines abelschen Zahlkörpers', *J. reine angew. Math.* **201** (1959), 119–149.
[8] T. Okada, 'On an extension of a theorem of S. Chowla', *Acta Arith.* **38**(4) (1980/81), 341–345.
[9] R. Schertz, 'Galoismodulstruktur und elliptische Funktionen', *J. Number Theory* **39**(3) (1991), 285–326.
[10] G. Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions* (Iwanami Shoten and Princeton University Press, Princeton, NJ, 1971).
[11] M. J. Taylor, 'Relative Galois module structure of rings of integers and elliptic functions II', *Ann. of Math. (2)* **121**(3) (1985), 519–535.
[12] B. L. van der Waerden, *Algebra I* (Springer, New York, 1991).

JA KYUNG KOO, Department of Mathematical Sciences,
KAIST, Daejeon 34141, 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 17035, Republic of Korea
e-mail: dhshin@hufs.ac.kr

DONG SUNG YOON, Department of Mathematical Sciences,
KAIST, Daejeon 34141, Republic of Korea
e-mail: math_dsyoon@kaist.ac.kr