Bull. Aust. Math. Soc. (First published online 2024), page 1 of 12*
doi:10.1017/S0004972724000339
*Provisional—final page numbers to be inserted when paper edition is published

NORMAL BASES FOR FUNCTION FIELDS

YOSHINORI HAMAHATA

(Received 8 September 2023; accepted 2 April 2024)

Abstract

In function fields in positive characteristic, we provide a concrete example of completely normal elements for a finite Galois extension. More precisely, for a nonabelian extension, we construct completely normal elements for Drinfeld modular function fields using Siegel functions in function fields. For an abelian extension, we construct completely normal elements for cyclotomic function fields.

2020 *Mathematics subject classification*: primary 11F52; secondary 11G16, 11R60, 12F05.

Keywords and phrases: normal basis, Drinfeld modular function field, Siegel function, cyclotomic function field.

1. Introduction

Let E be a finite Galois extension of a field F. The normal basis theorem (see [1]) states that there exists an element $a \in E$ such that $\{\sigma(a) \mid \sigma \in \mathrm{Gal}(E/F)\}$ is a basis of E over F. This basis is referred to as a *normal basis* for E/F, and the element a is referred to as *normal* in E/F. Blessenohl and Johnson [3] proved that there exists a primitive element a for E/F such that a is normal in E/L for each intermediate field L of E/F. This element a is referred to as *completely normal* in E/F. When F is infinite, little is known about explicit constructions of completely normal elements. For examples in the context of number fields and abelian function fields of characteristic zero, we refer to [8, 13, 14, 16] and [10], respectively.

For a positive integer N, the group

$$\Gamma(N) = \left\{ \sigma \in \mathrm{SL}_2(\mathbb{Z}) \,\middle|\, \sigma \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod N \right\},$$

which is the principal congruence subgroup of $\Gamma(1) = \mathrm{SL}_2(\mathbb{Z})$ of level N, acts on the classical upper-half plane $\mathfrak{H} = \{z \in \mathbb{C} \mid \mathrm{Im}(z) > 0\}$ using fractional linear transformations. Let $\mathbb{C}(X(N))$ be the modular function field for the classical modular

This work was supported by JSPS KAKENHI Grant Number 21K03192.

https://doi.org/10.1017/S0004972724000339 Published online by Cambridge University Press

curve $X(N)$ for $\Gamma(N)$. It is known that $\mathbb{C}(X(N))$ is a finite Galois extension of $\mathbb{C}(X(1))$ with

$$\mathrm{Gal}(\mathbb{C}(X(N))/\mathbb{C}(X(1))) \cong \Gamma(1)/\pm\Gamma(N) \cong \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I_2\}.$$

For $v = (v_1, v_2) \in \mathbb{Q}^2 \setminus \mathbb{Z}^2$, the classical Siegel function $s_v(z)$ for $z \in \mathfrak{H}$ is defined as follows. For $z \in \mathfrak{H}$, we set $\tau = v_1 z + v_2$. Let $\eta(\tau, [z, 1])$ and $\sigma(\tau, [z, 1])$ be the Weierstrass eta- and sigma-functions for the lattice $[z, 1] = \mathbb{Z}z + \mathbb{Z}$, respectively. We define the Klein form $k_v(z)$ by $k_v(z) = \exp(-\eta(\tau, [z, 1])\tau/2)\sigma(\tau, [z, 1])$ and the Siegel function $s_v(z)$ by

$$s_v(z) = k_v(z)\eta^2(z),$$

where $\eta(z)$ denotes the Dedekind eta-function. It is known that $s_v(z)$ belongs to $\mathbb{C}(X(N))$. (For further details, we refer to [12].) Koo *et al.* [11] provided a completely normal element in $\mathbb{C}(X(N))/\mathbb{C}(X(1))$ in terms of the Siegel functions.

The purpose of this paper is to provide a concrete example of completely normal elements for a finite Galois extension of function fields in positive characteristic. More precisely, for a nonabelian extension, using Siegel functions in function fields, we construct completely normal elements for Drinfeld modular function fields. For an abelian extension, we construct completely normal elements for cyclotomic function fields.

The remainder of this paper is organised as follows. In Section 2, on the basis of Artin's argument in [1], we provide a criterion for completely normal elements. Section 3 is devoted to an overview of A-lattices and Drinfeld A-modules to prepare for Section 4. In Section 4, we study Siegel functions in function fields and provide a product formula for Siegel functions. In Sections 5 and 6, we construct completely normal elements for a nonabelian finite Galois extension of Drinfeld modular function fields, applying the product formula in the previous section, and for cyclotomic function fields, respectively.

2. A criterion for completely normal elements

Let $A = \mathbb{F}_q[T]$ be the polynomial ring over $\mathbb{F}_q$, a finite field with q elements. Let $K = \mathbb{F}_q(T)$ and $K_\infty = \mathbb{F}_q((1/T))$ denote the quotient field of A and the completion of K at $\infty = (1/T)$, respectively. Let $\mathbb{C}_\infty$ be the completion of an algebraic closure of K_∞ and let A_+ be the set of monic elements in A. We write $\Omega = \mathbb{C}_\infty \setminus K_\infty$ for the Drinfeld upper-half plane. Let $|\cdot|$ be the absolute value of $\mathbb{C}_\infty$ normalised by $|T| = q$.

Let F be a field containing K and let E be a finite Galois extension of F. To find a completely normal element in E/F, we use Artin's argument in [1]. Let L be any intermediate field of E/F and set $G = \mathrm{Gal}(E/L) = \{\sigma_1 = 1, \ldots, \sigma_s\}$. Let g be a primitive element of E over F and let $\alpha(x)$ be the minimal polynomial for g over L with $\deg \alpha(x) = s$. For each $\sigma \in G$, set $\beta_\sigma(x) = \alpha(x)/(x - g^\sigma)$. Moreover, let

$$D(x) = \det(\beta_{\sigma_i\sigma_j^{-1}}(x)).$$

https://doi.org/10.1017/S0004972724000339 Published online by Cambridge University Press

From the definition of β_σ,

$$D(g) = \begin{vmatrix} \beta_1(g) & 0 & \cdots & 0 \\ 0 & \beta_1(g) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \beta_1(g) \end{vmatrix} = \beta_1(g)^s \neq 0,$$

which implies that $D(x)$ is not zero.

We have the following criterion for completely normal elements in E/F.

THEOREM 2.1. *Let g be a primitive element of E over F. If $D(T^m)$ is nonzero for a positive integer m, then*

$$\frac{1}{T^m - g}$$

is completely normal in E/F.

PROOF. First, $\det((T^m - g^{\sigma_i\sigma_j^{-1}})^{-1})$ is nonzero because

$$D(T^m) = \alpha(T^m)^s \det\Big(\frac{1}{T^m - g^{\sigma_i\sigma_j^{-1}}}\Big).$$

By setting $J_m = (T^m - g)^{-1}$, we prove that the J_m^σ $(\sigma \in G)$ are linearly independent over L. Let $\Sigma_{\sigma\in G} x_\sigma J_m^\sigma = 0$ $(x_\sigma \in L)$. By letting $\tau^{-1} \in G$ act in this equation,

$$\sum_{i=1}^{s} x_{\sigma_i} J_m^{\sigma_i\sigma_j^{-1}} = 0 \quad (j = 1, \ldots, s)$$

for $\tau = \sigma_1, \ldots, \sigma_s$. As the determinant of the coefficients of these equations is $\det((T^m - g^{\sigma_i\sigma_j^{-1}})^{-1})$, it follows that $x_\sigma = 0$ for $\sigma \in G$. □

3. Overview of A-lattices and Drinfeld A-modules

We present an overview of A-lattices and Drinfeld A-modules. Further details can be found from Goss [7] and Rosen [15]. A rank r *A-lattice* Λ in $\mathbb{C}_\infty$ is a finitely generated A-submodule of rank r in $\mathbb{C}_\infty$ that is discrete in the topology of $\mathbb{C}_\infty$. For such an A-lattice Λ, we define the product

$$e_\Lambda(z) = z \prod_{0\neq\lambda\in\Lambda} \Big(1 - \frac{z}{\lambda}\Big).$$

This product converges uniformly on bounded sets in $\mathbb{C}_\infty$ and defines a map e_Λ such that $e_\Lambda : \mathbb{C}_\infty \to \mathbb{C}_\infty$. The map e_Λ has the following properties:

(E1) e_Λ is entire in the rigid analytic sense and is surjective;
(E2) e_Λ is $\mathbb{F}_q$-linear and Λ-periodic;
(E3) e_Λ has simple zeros at the points of Λ and no other zeros.

https://doi.org/10.1017/S0004972724000339 Published online by Cambridge University Press

For every $a \in A$, there exists a unique polynomial $\phi_a = \phi_a^\Lambda$ of the form $\sum l_i(a) z^{q^i}$ such that $\phi_a(e_\Lambda(z)) = e_\Lambda(az)$. Let $\tau = z^q$ and $\mathbb{C}_\infty\{\tau\}$ be the noncommutative ring in τ with the commutation rule $c^q \tau = \tau c$ $(c \in \mathbb{C}_\infty)$. There exists a unique positive integer r such that

$$\phi_a = \sum_{i=0}^{r \deg a} l_i(a) \tau^i \quad (l_0(a) = a, l_{r \deg a}(a) \neq 0)$$

for any $a \in A \setminus \{0\}$. The map $\phi : A \to \mathbb{C}_\infty\{\tau\}$, $a \mapsto \phi_a$ is then called a *Drinfeld A-module* of rank r over $\mathbb{C}_\infty$. Because ϕ is an $\mathbb{F}_q$-linear ring homomorphism, the values ϕ_a $(a \in A)$ are determined by ϕ_T. The rank one Drinfeld A-module $\rho : A \to \mathbb{C}_\infty\{\tau\}$ defined by $\rho_T(z) = Tz + z^q$ is called the *Carlitz module* and the rank one A-lattice $L = \bar{\pi} A$ corresponding to ρ is analogous to $2\pi i \mathbb{Z}$. It is well known that there is a one-to-one correspondence between the set of A-lattices of rank r and the set of Drinfeld A-modules of rank r over $\mathbb{C}_\infty$. This correspondence is given by $\phi_a(e_\Lambda(z)) = e_\Lambda(az)$ for all $a \in A$.

4. Siegel functions

This section discusses Siegel functions.

4.1. Basic results. For $\omega \in \Omega$, let $\Lambda_\omega = A\omega + A$ be the rank two A-lattice. For the rank two Drinfeld A-module $\phi^{\Lambda_\omega} : A \to \mathbb{C}_\infty\{\tau\}$ corresponding to Λ_ω,

$$\phi_T^{\Lambda_\omega} = T + g(\omega)\tau + \Delta(\omega)\tau^2. \tag{4.1}$$

The function Δ is called the Drinfeld discriminant function and is a Drinfeld cusp form of weight $q^2 - 1$ for the Drinfeld modular group $\Gamma(1) = GL_2(A)$. Let ρ and $L = \bar{\pi} A$ be the Carlitz module and the corresponding rank one A-lattice, respectively. Considering ρ_a $(a \in A)$ to be a polynomial in x, we set

$$f_a(x) = \rho_a(x^{-1}) x^{|a|},$$

which is called the ath *inverse cyclotomic polynomial*. Let $t(\omega) = e_L(\bar{\pi}\omega)^{-1}$. Gekeler [5] established a product formula for Δ.

THEOREM 4.1 (Gekeler). *The function Δ has the product expansion*

$$\Delta(\omega) = -\bar{\pi}^{q^2-1} t^{q-1} \prod_{0 \neq a \in A} f_a(t)^{q^2-1}$$

with a positive radius of convergence for t.

Let

$$\eta(\omega) = \bar{\pi} t^{1/(q+1)} \prod_{0 \neq a \in A} f_a(t).$$

Thus, $\eta^{q^2-1} = -\Delta$.

https://doi.org/10.1017/S0004972724000339 Published online by Cambridge University Press

We take $n \in A_+$ with $\deg n > 0$. For $u = (u_1, u_2) \in (n^{-1}A/A)^2$, let

$$e_u(\omega) = e_{\Lambda_\omega}(u_1\omega + u_2).$$

The *Siegel function* g_u is formally defined as

$$g_u(\omega) = e_u(\omega)\eta(\omega).$$

The group $\Gamma(1)$ acts on Ω by $\sigma\omega = (a\omega + b)(c\omega + d)^{-1}$ for $\sigma = (\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}) \in \Gamma(1)$ and $\omega \in \Omega$. The *principal congruence subgroup* of level n is

$$\Gamma(n) = \left\{\sigma \in \Gamma(1) \,\middle|\, \sigma \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod n\right\}.$$

A congruence subgroup with conductor n of $\Gamma(1)$ is a subgroup Γ containing $\Gamma(n)$. For this congruence subgroup Γ, the rigid analytic space $\Gamma \setminus \Omega$ is endowed with a smooth affine algebraic curve over $\mathbb{C}_\infty$. The curve X_Γ, which is a smooth projective model of $\Gamma \setminus \Omega$, is the Drinfeld modular curve for Γ. Let $X(n)$ and $X(1)$ be Drinfeld modular curves for $\Gamma(n)$ and $\Gamma(1)$, respectively. In addition, let $\mathbb{C}_\infty(X(n))$ and $\mathbb{C}_\infty(X(1))$ be the meromorphic function fields of $\Gamma(n)$ and $\Gamma(1)$, respectively. The group $\Gamma(1)$ acts on $\mathbb{C}_\infty(X(n))$ by $h^\sigma(\omega) = h(\sigma\omega)$ for $h \in \mathbb{C}_\infty(X(n))$ and $\sigma \in \Gamma(1)$. It is known that $\mathbb{C}_\infty(X(n))/\mathbb{C}_\infty(X(1))$ is a Galois extension with

$$\mathrm{Gal}(\mathbb{C}_\infty(X(n))/\mathbb{C}_\infty(X(1))) \cong \Gamma(1)/Z(\mathbb{F}_q)\Gamma(n), \tag{4.2}$$

whose order is $|n|^3 \prod_{P|n}(1 - 1/|P|^2)$, where $Z(\mathbb{F}_q)$ denotes the $\mathbb{F}_q$-valued scalar matrices, and the product $\prod_{P|n}$ is taken over all monic irreducibles P that divide n. (See [6] for further details.)

Let $t_n(\omega) = e_L(\bar{\pi}\omega/n)^{-1}$, which is a parameter at ∞ for $X(n)$.

Proposition 4.2 (Gekeler [4]). *Let $n \in A_+$ with $\deg n > 0$ and $u = (n^{-1}s_1, n^{-1}s_2) \in (n^{-1}A/A)^2$ with $\deg s_1, \deg s_2 < \deg n$. Then, the following statements hold.*

(i) *The order of $g_u(\omega)$ at t_n is given by*

$$\mathrm{ord}_{t_n} g_u(\omega) = |n|\left(\frac{1}{q+1} - \frac{|s_1|}{|n|}\right).$$

(ii) *For $\sigma \in \Gamma(1)$, $g_u^\sigma = g_{u\sigma}$.*

(iii) *For a subset S of $(n^{-1}A/A)^2$, the product $\prod_{u\in S} g_u^{m(u)}$ belongs to $\mathbb{C}_\infty(X(n))$ if and only if $\sum_{u\in S} m(u) \equiv 0 \pmod{q+1}$.*

We establish the following product formula for the Siegel function g_u.

Theorem 4.3 (A product formula). *Let $n \in A_+$ with $\deg n > 0$. For $u = (n^{-1}s_1, n^{-1}s_2) \in (n^{-1}A/A)^2$, g_u has the product expansion*

https://doi.org/10.1017/S0004972724000339 Published online by Cambridge University Press

$$g_u(\omega) = -t_n^{|n|/(q+1)-|s_1|} f_n(t_n)^{-1/(q+1)}(f_{-s_1}(t_n) - e_L(\bar{\pi}s_2/n)t_n^{|s_1|}) \\ \times \prod_{0\neq a\in A}(f_{na-s_1}(t_n) - e_L(\bar{\pi}s_2/n)t_n^{|na|})$$

with a positive radius of convergence for t_n.

Remark 4.4. The classical Siegel function $s_v(z)$ introduced in Section 1 has the following product expansion:

$$s_v(z) = -e^{\pi i v_2(v_1-1)}q^{B_2(v_1)/2}(1-q^{v_1}e^{2\pi i v_2})\prod_{m=1}^{\infty}(1-q^{m+v_1}e^{2\pi i v_2})(1-q^{m-v_1}e^{-2\pi i v_2}),$$

where $q = e^{2\pi i z}$ and $B_2(x) = x^2 - x + 1/6$.

4.2. Proof of Theorem 4.3. Using [4, (2.1)],

$$e_u(\omega) = \bar{\pi}^{-1}t_n^{-|s_1|}(f_{s_1}(t_n) + e_L(\bar{\pi}s_2/n)t_n^{|s_1|})\prod_{0\neq a\in A}\frac{f_{na-s_1}(t_n) - e_L(\bar{\pi}s_2/n)t_n^{|na|}}{f_{na}(t_n)}.$$

As $t = t_n^{|n|}/f_n(t_n)$, for $a \in A \setminus \{0\}$,

$$f_a(t) = \rho_{na}(e_L(\bar{\pi}\omega/n))t^{|a|} = \rho_{na}(e_L(\bar{\pi}\omega/n))\bigg(\frac{t_n^{|n|}}{f_n(t_n)}\bigg)^{|a|} = \frac{f_{na}(t_n)}{f_n(t_n)^{|a|}},$$

which yields

$$\eta(\omega) = \bar{\pi}t_n^{|n|/(q+1)}f_n(t_n)^{-1/(q+1)}\prod_{0\neq a\in A}\frac{f_{na}(t_n)}{f_n(t_n)^{|a|}}.$$

Therefore,

$$g_u(\omega) = -t_n^{|n|/(q+1)-|s_1|} f_n(t_n)^{-1/(q+1)}(f_{-s_1}(t_n) - e_L(\bar{\pi}s_2/n)t_n^{|s_1|}) \\ \times \prod_{0\neq a\in A}\frac{f_{na-s_1}(t_n) - e_L(\bar{\pi}s_2/n)t_n^{|na|}}{f_n(t_n)^{|a|}}.$$

To simplify this expression, the following lemma is required.

Lemma 4.5. *We have*

$$\prod_{a\in A} f_n(t_n)^{|a|} = 1.$$

Proof. For $a \in A$, let

$$W_a(t_n) = f_n(t_n)^{-|a|}\prod_{c\in\mathbb{F}_q} f_n(t_n)^{|aT+c|}.$$

Because

$$f_n(t_n)^{|a|}W_a(t_n) = \prod_{c\in\mathbb{F}_q} f_n(t_n)^{|aT+c|} \quad\text{and}\quad \prod_{\deg a\leq n} f_n(t_n)^{|a|}W_a(t_n) = \prod_{\deg a\leq n+1} f_n(t_n)^{|a|},$$

it follows that

$$\prod_{0\neq a\in A} f_n(t_n)^{|a|}W_a(t_n)=\prod_{0\neq a\in A} f_n(t_n)^{|a|},$$

which yields $\prod_{0\neq a\in A} W_a(t_n)=1$. From this,

$$\prod_{0\neq a\in A} f_n(t_n)^{|a|}=\prod_{0\neq a\in A}\prod_{c\in\mathbb{F}_q} f_n(t_n)^{|aT+c|}=\Big(\prod_{0\neq a\in A} f_n(t_n)^{|a|}\Big)^{q^2},$$

which yields $(\prod_{0\neq a\in A} f_n(t_n)^{|a|})^{q^2-1}=1$. Noting that $\prod_{0\neq a\in A} f_n(0)^{|a|}=1$, we have $\prod_{0\neq a\in A} f_n(t_n)^{|a|}=1$. □

From this lemma, the proof of Theorem 4.3 is completed.

5. Normal bases for Drinfeld modular function fields

In this section, we construct the completely normal elements in Drinfeld modular function fields.

5.1. The primitive element h_n. Using Siegel functions, we construct a primitive element of $\mathbb{C}_\infty(X(n))$ over $\mathbb{C}_\infty(X(1))$.

DEFINITION 5.1. We set

$$h_n=\frac{1}{g_{(0,n^{-1})}^{2q+1}g_{(n^{-1},0)}}.$$

The function h_n has the following properties.

PROPOSITION 5.2.

(i) *$h_n\in\mathbb{C}_\infty(X(n))$.*
(ii) *$h_n(\lambda\omega)=\lambda h_n(\omega)$ for $\lambda\in\mathbb{F}_q^*$.*

PROOF.

(i) This follows from Proposition 4.2(iii).
(ii) For $\lambda\in\mathbb{F}_q^*$ and $a\in A\setminus\{0\}$,

$$t(\lambda\omega)=\lambda^{-1}t(\omega),\quad f_a(t(\lambda\omega))=f_a(t(\omega)),\quad \eta(\lambda\omega)=\lambda^{-1/(q+1)}\eta(\omega),$$
$$g_{(0,n^{-1})}(\lambda\omega)=\lambda^{-1/(q+1)}g_{(0,n^{-1})}(\omega),\quad g_{(n^{-1},0)}(\lambda\omega)=\lambda^{q/(q+1)}g_{(n^{-1},0)}(\omega).$$

Thus, we obtain property (ii). □

LEMMA 5.3. *For $\sigma\in\Gamma(1)$, $\mathrm{ord}_{t_n}(h_n^{\sigma}/h_n)\geq 0$. Equality holds if and only if*

$$\sigma\equiv\begin{pmatrix}a_1 & *\\ 0 & d_1\end{pmatrix}\pmod{n},$$

where $a_1,d_1\in\mathbb{F}_q^*$.

https://doi.org/10.1017/S0004972724000339 Published online by Cambridge University Press

PROOF. Let $\sigma \equiv \left(\begin{smallmatrix} a_1 & b_1 \\ c_1 & d_1 \end{smallmatrix}\right) \pmod{n}$, where $a_1, b_1, c_1, d_1 \in A$, $\deg a_1, \deg b_1, \deg c_1, \deg d_1 < \deg n$. Using Proposition 4.2,

$$\mathrm{ord}_{t_n}(h_n^\sigma / h_n) = (2q+1)|c_1| + (|a_1| - 1).$$

Since $a_1 d_1 - b_1 c_1 \in \mathbb{F}_q^*$, either $a_1 \neq 0$ or $c_1 \neq 0$.

(i) When $a_1 \neq 0$ and $c_1 \neq 0$, $(2q+1)|c_1| + (|a_1| - 1) > 0$.
(ii) When $a_1 = 0$ and $c_1 \neq 0$, $(2q+1)|c_1| + (|a_1| - 1) \geq 2q > 0$.
(iii) When $a_1 \neq 0$ and $c_1 = 0$, $(2q+1)|c_1| + (|a_1| - 1) = |a_1| - 1 \geq 0$,

which yields the first part of the lemma.

For the latter part of the lemma, we use item (iii). Equality holds if and only if $c_1 = 0, a_1 \in \mathbb{F}_q^*$, which is equivalent to $c \in nA$ and $a_1, d_1 \in \mathbb{F}_q^*$. □

PROPOSITION 5.4. *The function h_n generates $\mathbb{C}_\infty(X(n))$ over $\mathbb{C}_\infty(X(1))$.*

PROOF. We assume that $\sigma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma(1)$ leaves h_n fixed. Because $\mathrm{ord}_{t_n} h_n^\sigma = \mathrm{ord}_{t_n} h_n$, Lemma 5.3 implies that

$$a \equiv a_1, \ c \equiv 0, \ d \equiv d_1 \pmod{n}, \quad a_1, d_1 \in \mathbb{F}_q^*.$$

For $\tau = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$, $\mathrm{ord}_{t_n} h_n^{\sigma\tau} = \mathrm{ord}_{t_n} h_n^\tau$, which yields

$$|n|\Big[(2q+1)\Big(\frac{1}{|n|} - \frac{1}{q+1}\Big) + \Big(\frac{|b_1|}{|n|} - \frac{1}{q+1}\Big)\Big] = |n|\Big[(2q+1)\Big(\frac{1}{|n|} - \frac{1}{q+1}\Big) + \Big(-\frac{1}{q+1}\Big)\Big]$$

by Proposition 4.2. In this expression, $b_1 \in A$ is defined by $b \equiv b_1 \pmod{n}, \deg b_1 < \deg n$. Hence, $b_1 = 0$ and $\sigma \equiv \left(\begin{smallmatrix} a_1 & 0 \\ 0 & d_1 \end{smallmatrix}\right) \pmod{n}$. By letting $\gamma = \sigma\left(\begin{smallmatrix} a_1^{-1} & 0 \\ 0 & d_1^{-1} \end{smallmatrix}\right)$, we observe that $\gamma \in \Gamma(n)$. Using Proposition 4.2,

$$h_n = h_n^\sigma = h_n^{\gamma\left(\begin{smallmatrix} a_1 & 0 \\ 0 & d_1 \end{smallmatrix}\right)} = h_n^{\left(\begin{smallmatrix} a_1 & 0 \\ 0 & d_1 \end{smallmatrix}\right)} = \frac{a_1}{d_1} h_n.$$

Hence, $\sigma = \left(\begin{smallmatrix} a_1 & 0 \\ 0 & a_1 \end{smallmatrix}\right)\gamma \in Z(\mathbb{F}_q)\Gamma(n)$. Using (4.2) and Galois theory, the proof of this proposition is completed. □

REMARK 5.5. It is known that

$$\mathbb{C}_\infty(X(1)) = \mathbb{C}_\infty(j), \quad \mathbb{C}_\infty(X(n)) = \mathbb{C}_\infty(j, f_u \mid u \in (n^{-1}A/A)^2),$$

where j is the modular function defined by $j(\omega) = g(\omega)^{q+1}/\Delta(\omega)$ using g, Δ in (4.1), and f_u is the Fricke function defined by $f_u(\omega) = g(\omega)e_u(\omega)^{q-1}$. From Proposition 5.4, we obtain $\mathbb{C}_\infty(X(n)) = \mathbb{C}_\infty(j, h_n)$.

The following lemma is required in the next subsection.

LEMMA 5.6. *Let l be a positive integer. If*

$$q^{-2l} < |t_n| \leq q^{-l-1/(q-1)}, \tag{5.1}$$

then

$$|h_n^{-1}(\sigma\omega)| < q^{4ql|n|+6}$$

for any $\sigma \in \Gamma(1)$.

PROOF. Let $\sigma \equiv \left(\begin{smallmatrix} a_1 & b_1 \\ c_1 & d_1 \end{smallmatrix}\right) \pmod{n}$, where $a_1, b_1, c_1, d_1 \in A$, $\deg a_1, \deg b_1, \deg c_1, \deg d_1 < \deg n$. By Proposition 4.2(ii) and Theorem 4.3,

$$\begin{aligned} h_n^{-1}(\sigma\omega) = {} & t_n^{(|n|-|a_1|)+(|n|-|c_1|)-2q|c_1|} f_n(t_n)^{-2} \\ & \times (f_{-c_1}(t_n) - e_L(\bar{\pi} d_1/n) t_n^{|c_1|})^{2q+1} (f_{-a_1}(t_n) - e_L(\bar{\pi} b_1/n) t_n^{|a_1|}) \\ & \times \prod_{0 \neq a \in A} (f_{na-c_1}(t_n) - e_L(\bar{\pi} d_1/n) t_n^{|na|})^{2q+1} (f_{na-a_1}(t_n) - e_L(\bar{\pi} b_1/n) t_n^{|na|}). \end{aligned}$$

Gekeler [5, Lemma 1] proved that if t_n satisfies (5.1) and $a \in A \setminus \{0\}$ with $\deg a = d$, then $|f_a(t_n) - 1| \leq (q^{-l})^{q^{d-1}(q-1)}$. For $e_L(\bar{\pi} d_1/n)$,

$$|e_L(\bar{\pi} d_1/n)| = |\bar{\pi} e_A(d_1/n)| = q^{q/(q-1)+\deg d_1 - \deg n} \leq q^{1/(q-1)}.$$

Similarly, we find that $|e_L(\bar{\pi} b_1/n)| \leq q^{1/(q-1)}$. Therefore,

$$|h_n^{-1}(\sigma\omega)| \leq |t_n|^{-2q|c_1|} |f_{-c_1}(t_n) - e_L(\bar{\pi} d_1/n) t_n^{|c_1|}|^{2q+1} |f_{-a_1}(t_n) - e_L(\bar{\pi} b_1/n) t_n^{|a_1|}|.$$

We have

$$\begin{aligned} |t_n|^{-2q|c_1|} &< (q^{-2l})^{-2q|n|}, \\ |f_{-c_1}(t_n) - e_L(\bar{\pi} d_1/n) t_n^{|c_1|}|^{2q+1} &\leq q^{(2q+1)/(q-1)}, \\ |f_{-a_1}(t_n) - e_L(\bar{\pi} b_1/n) t_n^{|a_1|}| &\leq q^{1/(q-1)}, \end{aligned}$$

which yields the lemma. □

5.2. Completely normal elements. Using h_n, we construct completely normal elements in $\mathbb{C}_\infty(X(n))/\mathbb{C}_\infty(X(1))$. Let $r = [\mathbb{C}_\infty(X(n)) : \mathbb{C}_\infty(X(1))]$.

THEOREM 5.7. *Let g be a primitive element of $\mathbb{C}_\infty(X(n))$ over $\mathbb{C}_\infty(X(1))$ and let $0 < \delta_2 < \delta_1 < 1$. We assume that there exists a positive constant $M \geq 1$ such that $|g(\omega)| < M$ for $\delta_2 < |t_n(\omega)| < \delta_1$. If $m > \log_q M^{r(r-1)}$, then*

$$\frac{1}{T^m - g}$$

is completely normal in $\mathbb{C}_\infty(X(n))/\mathbb{C}_\infty(X(1))$.

PROOF. Let L be any intermediate field of $\mathbb{C}_\infty(X(n))/\mathbb{C}_\infty(X(1))$, and set

$$G = \mathrm{Gal}(\mathbb{C}_\infty(X(n))/L) = \{\sigma_1 = 1, \ldots, \sigma_s\}.$$

If $\alpha(x)$ is the minimal polynomial for g over L, then $\deg \alpha(x) = s$. For each $\sigma \in G$, set $\beta_\sigma(x) = \alpha(x)/(x - g^\sigma)$. Moreover, let $D(x) = \det(\beta_{\sigma_i \sigma_j^{-1}}(x))$. For $\omega \in \Omega$ with

https://doi.org/10.1017/S0004972724000339 Published online by Cambridge University Press

$\delta_2 < |t_n(\omega)| < \delta_1$, we set

$$\beta_\sigma(x,\omega) = \prod_{\gamma \in G \setminus \{\sigma\}} (x - g^\gamma(\omega)) \quad \text{and} \quad D(x,\omega) = \det(\beta_{\sigma_i \sigma_j^{-1}}(x,\omega)).$$

As the coefficients of $\beta_\sigma(x,\omega)$ are sums of products of $g^\gamma(\omega)$ $(\gamma \in G \setminus \{\sigma\})$, the absolute value of each of these coefficients is not greater than M^{s-1}. Hence, the absolute value of each coefficient of $D(x,\omega)$ is not greater than $M^{s(s-1)}$. If $m > \log_q M^{r(r-1)}$, then $q^m > M^{s(s-1)}$. When $D(x,\omega) = \sum_{i=0}^{s(s-1)} a_i x^i$, the absolute value of a nonzero a_i satisfies $|a_i| \le M^{s(s-1)} < q^m$, which implies that $q^{mi} \le |a_i T^{mi}| < q^{m(i+1)}$. Thus, $|D(T^m,\omega)|$ is nonzero, implying that $D(T^m)$ is also nonzero. Therefore, the theorem follows from Theorem 2.1. □

DEFINITION 5.8. For a positive integer m, we set

$$H_{n,m} = \frac{h_n}{T^m h_n - 1}.$$

The function $H_{n,m}$ belongs to $\mathbb{C}_\infty(X(n))$. The following theorem is a consequence of Theorem 5.7.

THEOREM 5.9. *If $m > 2r(r-1)(2q|n|+1)$, then the element $H_{n,m}$ is completely normal in $\mathbb{C}_\infty(X(n))/\mathbb{C}_\infty(X(1))$.*

PROOF. Using Proposition 5.4, h_n^{-1} is a primitive element of $\mathbb{C}_\infty(X(n))$ over $\mathbb{C}_\infty(X(1))$. Taking a positive integer $l > 2$, let $\delta_1 = q^{-l-2}$ and $\delta_2 = q^{-2l}$. If $\delta_2 < |t_n| < \delta_1$, then we have $|h_n^{-1}(\sigma\omega)| < q^{4ql|n|+6}$ for $\sigma \in \Gamma(1)$ using Lemma 5.6. Applying Theorem 5.7 for $M = q^{4ql|n|+6}$ and $g = h_n^{-1}$, we obtain the theorem. □

6. Normal bases for cyclotomic function fields

In this section, we construct completely normal elements in cyclotomic function fields and their maximal real subfields.

Let ρ be the Carlitz module. For $n \in A_+$, let $\rho[n] = \{\alpha \in \mathbb{C}_\infty \mid \rho_n(\alpha) = 0\}$ be the set of Carlitz n-torsion points. The set $\rho[n]$ is a cyclic A-module and its generator is called the *primitive Carlitz n-torsion point*. The minimal polynomial $\Phi_n(x)$ for any primitive n-torsion point over K is called the *Carlitz* nth *cyclotomic polynomial*. The polynomials $\rho_n(x)$ and $\Phi_n(x)$ have degrees $q^{\deg n}$ and $\varphi(n)$, respectively, where $\varphi(n) := \#(A/nA)^*$. (For further details on these polynomials, we refer to [3].) For the primitive Carlitz n-torsion point λ_n, let $K_n = K(\lambda_n)$ be the field generated over K by adjoining λ_n. If $\sigma \in \mathrm{Gal}(K_n/K)$, then $\sigma(\lambda_n)$ is another primitive Carlitz n-torsion point. Hence, there exists $a \in A$ with $\gcd(a,n) = 1$ such that $\sigma(\lambda_n) = \rho_a(\lambda_n)$. Let $\epsilon_a = \sigma$. The correspondence $\epsilon_a \mapsto a$ induces the isomorphism $\mathrm{Gal}(K_n/K) \xrightarrow{\sim} (A/nA)^*$ (see [15, Theorem 12.8]).

https://doi.org/10.1017/S0004972724000339 Published online by Cambridge University Press

THEOREM 6.1. *Let F be a finite Galois extension of K of degree r contained in $\mathbb{C}_\infty$ and let μ be a primitive element of F over K with $|\mu| \le M$, where $M \ge 1$ is a constant. If $m > \log_q M^{r(r-1)}$, then*

$$\frac{1}{T^m - \mu}$$

is completely normal in F/K.

PROOF. Let L be any intermediate field of F/K and $G = \mathrm{Gal}(F/L) = \{\sigma_1 = 1, \ldots, \sigma_s\}$. If $\alpha(x)$ is the minimal polynomial of μ over L, then $\deg \alpha(x) = s$. For each $\sigma \in G$, we set $\beta_\sigma(x) = \alpha(x)/(x - \mu^\sigma)$. Moreover, we set $D(x) = \det(\beta_{\sigma_i\sigma_j^{-1}}(x))$. As the coefficients of $\beta_\sigma(x)$ are sums of products of μ^γ ($\gamma \in G \setminus \{\sigma\}$), the absolute value of each of their coefficients is not greater than M^{s-1}. Hence, the absolute value of each coefficient of $D(x)$ is not greater than $M^{s(s-1)}$. If $m > \log_q M^{r(r-1)}$, then $q^m > M^{s(s-1)}$. When $D(x) = \sum_{i=0}^{s(s-1)} a_i x^i$, the absolute value of a nonzero a_i satisfies $|a_i| \le M^{s(s-1)} < q^m$, which implies that $q^{mi} \le |a_i T^{mi}| < q^{m(i+1)}$. Hence, $|D(T^m)|$ is nonzero. Therefore, the theorem follows from Theorem 2.1. □

For a completely normal element in K_n/K, we have the following result.

THEOREM 6.2. *For a monic element $n \in A_+$ with $\deg n > 0$, let K_n be the cyclotomic function field determined by n. For any positive integer m,*

$$\frac{1}{T^m - e_L(\bar{\pi}/n)}$$

is completely normal in K_n/K.

PROOF. According to [15], $e_L(\bar{\pi}/n)$ is a primitive element of K_n over K. When $\mu = e_L(\bar{\pi}/n)$, $|\mu| = |\bar{\pi} e_A(1/n)| = q^{q/(q-1)-\deg n} \le q^{1/(q-1)}$. When $M = q^{1/(q-1)}$, $\log_q M^{r(r-1)} = 1/(q-1) < 1$. Therefore, the theorem follows from Theorem 6.1. □

Let K_n^+ be the fixed field of $\{\epsilon_a \in \mathrm{Gal}(K_n/K) \mid a \in \mathbb{F}_q^*\}$. This field is referred to as the *maximal real subfield* of K_n. For a completely normal element in K_n^+/K, we have the following result.

THEOREM 6.3. *Notation being as in Theorem 6.2, we let $r = [K_n^+ : K]$. If $m > r(r-1)$, then*

$$\frac{1}{T^m - e_L(\bar{\pi}/n)^{q-1}}$$

is completely normal in K_n^+/K.

PROOF. According to [15], $e_L(\bar{\pi}/n)^{q-1}$ is a primitive element of K_n^+ over K. When $\mu = e_L(\bar{\pi}/n)^{q-1}$, we have $|\mu| = |\bar{\pi} e_A(1/n)|^{q-1} \le q$. When $M = q$, $\log_q M^{r(r-1)} = r(r-1)$. Therefore, the theorem follows from Theorem 6.1. □

https://doi.org/10.1017/S0004972724000339 Published online by Cambridge University Press

REMARK 6.4. For $n \in A_+$ with $\deg n > 0$, let $R_n = \{a \in A_+ \mid \deg a < \deg n, \gcd(a, n) = 1\}$. In [9], we proved that

$$G_k(e_L(\bar{\pi}a/n)^{-1}) \quad (a \in R_n)$$

are linearly independent over K for any positive integer k, where $G_k(x)$ is the kth Goss polynomial of $L = \bar{\pi}A$. It is known that $G_{q-1}(x) = x^{q-1}$. As $\{1/e_L(\bar{\pi}a/n)^{q-1} \mid a \in R_n\}$ is contained in K_n^+, $\{\epsilon_(1/e_L(\bar{\pi}/n)^{q-1}) \mid a \in R_n\} = \{1/e_L(\bar{\pi}a/n)^{q-1} \mid a \in R_n\}$ is a normal basis for K_n^+/K. This is analogous to the result provided by Okada [14].

Acknowledgement

The author would like to thank the anonymous referee for careful reading and the helpful comments that improved this paper.

References

[1] E. Artin, *Galois Theory* (Dover, New York, 1997).

[2] S. Bae, 'The arithmetic of Carlitz polynomials', *J. Korean Math. Soc.* **35** (1998), 341–260.

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

[4] E.-U. Gekeler, 'Modulare Einheiten für Functionenkörper', *J. reine angew. Math.* **348** (1984), 94–115.

[5] E.-U. Gekeler, 'A product expansion for the discriminant function of Drinfeld modules of rank two', *J. Number Theory* **21** (1985), 135–140.

[6] E.-U. Gekeler, *Drinfeld Modular Curves*, Lecture Notes in Mathematics, 1231 (Springer, Berlin–Heidelberg, 1986).

[7] D. Goss, *Basic Structures of Function Fields* (Springer, Berlin–Heidelberg, 1996).

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

[9] Y. Hamahata, 'Chowla's theorem over function fields', *Int. J. Number Theory* **14** (2018), 1689–1698.

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

[11] J. K. Koo, D. H. Shin and D. S. Yoon, 'Normal bases for modular function fields', *Bull. Aust. Math. Soc.* **95** (2017), 384–392.

[12] D. Kubert and S. Lang, *Modular Units* (Springer, New York, 1981).

[13] H.-W. Leopoldt, 'Über die Hauptordnung der ganzen Elemente eines abelschen Zahlkörpers', *J. reine angew. Math.* **201** (1959), 119–149.

[14] T. Okada, 'On an extension of a theorem of S. Chowla', *Acta Arith.* **38** (1980/81), 341–345.

[15] M. Rosen, *Number Theory in Function Fields* (Springer, New York, 2002).

[16] R. Schertz, 'Galoismodulstruktur und elliptische Funktionen', *J. Number Theory* **39** (1991), 285–326.

YOSHINORI HAMAHATA, Department of Applied Mathematics
Okayama University of Science, Ridai-cho 1-1, Okayama 700-0005, Japan
e-mail: hamahata@ous.ac.jp

https://doi.org/10.1017/S0004972724000339 Published online by Cambridge University Press