J. Austral. Math. Soc. **70** (2001), 56–70

BASES FOR CYCLOTOMIC UNITS OVER FUNCTION FIELDS

S. BAE and H. JUNG

(Received 15 February 1999; revised 11 April 2000)

Communicated by W. W. L. Chen

Abstract

We find a basis for the universal punctured even distribution and then a basis for the cyclotomic units over function fields.

2000 *Mathematics subject classification*: primary 11R58, 11R60.

0. Introduction

In the classical case, the structure of the group of cyclotomic units can be obtained from the universal punctured even distribution [6]. Gold and Kim [2] have found an explicit basis (a minimal set of generators) of the universal punctured even distribution and then, by eliminating some generators of it, a basis of the group of cyclotomic units. They used this basis to show that $U_n^G = U_m$ for all $m|n$ where $G = \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}(\zeta_m))$, and U_n (respectively U_m) is the group of cyclotomic units in $\mathbb{Q}(\zeta_n)$ (respectively $\mathbb{Q}(\zeta_m)$).

Galovich and Rosen introduced the cyclotomic units in the cyclotomic function fields [3, 4] and the distribution theory over function fields [5]. Bae described the group structure of universal even (odd) punctured distribution [1]. In this paper, we find a basis of the universal even punctured distribution in function field and from this basis find a basis of the group of cyclotomic units in the cyclotomic function fields, following the ideas of Gold and Kim [2].

Throughout this paper we fix the following notation. Since the case $q = 2$ is not so interesting, we assume that $q > 2$.

Supported in part by KOSEF 98-0701-01-01-3.

Notation

$$\begin{aligned}
\mathbb{F}_q &= \text{ the finite field with } q \text{ elements},\\
R_T &= \mathbb{F}_q[T],\\
k &= \mathbb{F}_q(T),\\
R_T(M) &= (1/M)R_T/R_T, \text{ for a monic polynomial } M \text{ of } R_T,\\
\lambda_M &= \text{ a primitive } M\text{-th root of the } \textit{Carlitz} \text{ module } \rho,\\
\lambda_M^A &= \rho_A(\lambda_M),\\
\Phi(M) &= \text{ the Euler } \textit{totient} \text{ function},\\
\pi(M) &= \text{ the number of monic irreducible divisors of } M,\\
k_M &= k(\lambda_M) = \text{ the } M\text{-th cyclotomic function field over } k,\\
O_M &= \text{ the integral closure of } R_T \text{ in } k_M,\\
E_M &= \text{ the group of units of } O_M.
\end{aligned}$$

1. Preliminaries

Let V_M be the subgroup of $k_M^\times$ generated by

$$\left\{\lambda_M^A : A \in R_T/MR_T,\ A \not\equiv 0 \mod M\right\} \cup \mathbb{F}_q^\times, \tag{1}$$

and $U_M = E_M \cap V_M$ what is called the *group of cyclotomic units* of $k_M^\times$. It is well known [4] that U_M is of finite index in E_M, in particular, they have the same rank $\Phi(M)/(q-1) - 1$. There are relations among the elements of V_M

$$\lambda_M^{cA} = c\lambda_M^A, \tag{2}$$

$$\lambda_M^{AN} = \prod_R \lambda_M^{A+BR} \quad \text{if } BN = M, \tag{3}$$

where $c \in \mathbb{F}_q^\times$ and R runs over all the polynomials whose degrees are less than $\deg(N)$. We begin by finding a basis of the universal punctured even distribution $(\mathbf{A}_M^\circ)^+$, which is an abelian group with generators

$$\left\{g\left(\frac{A}{M}\right) : \frac{A}{M} \in R_T(M),\ \frac{A}{M} \neq 0\right\}$$

and relations

$$g\left(\frac{cA}{M}\right) = g\left(\frac{A}{M}\right), \tag{4}$$

$$g\left(\frac{A}{N}\right) = \sum_R g\left(\frac{A+RN}{M}\right) \quad \text{if } N|M \text{ and } \frac{A}{N} \neq 0. \tag{5}$$

https://doi.org/10.1017/S1446788700002275 Published online by Cambridge University Press

Define

$$\varphi : \left(\mathsf{A}_M^\circ\right)^+ \longrightarrow V_M/\mathbb{F}_q^\times$$

by $\varphi(g(A/M)) = \lambda_M^A \mod \mathbb{F}_q^\times$. From the relations (2)–(4) and (5), we can easily see that φ is a well-defined homomorphism.

In [1], Bae showed that

$$\left(\mathsf{A}_M^\circ\right)^+ \simeq \mathbb{Z}^{\Phi(M)/(q-1)+\pi(M)-1} \bigoplus \left(\mathbb{Z}/(q-1)\right)^{2^{\pi(M)-1}-\pi(M)}.$$

Therefore, we have the following theorem.

THEOREM 1.1. *There is a split exact sequence*

$$0 \longrightarrow (\mathbb{Z}/(q-1))^{2^{r-1}-r} \longrightarrow \left(\mathsf{A}_M^\circ\right)^+ \xrightarrow{\varphi} V_M/\mathbb{F}_q^\times \longrightarrow 0,$$

where φ is defined as above and $r = \pi(M)$.

2. Basis of $\left(\mathsf{A}_M^\circ\right)^+$

Let M be a monic polynomial and $Q_1^{e_1} Q_2^{e_2} \cdots Q_r^{e_r}$ be its factorization, with Q_i monic irreducible. Let

$$S = \{A \in R_T : \deg A < \deg M, A \text{ is relatively prime to } M\},$$

and define three subsets S_i, $\tilde{S}_i$ and S_i^* of S for each i as follows:

$$S_i = \{A \in S : A \equiv 1 \mod M/Q_i^{e_i}\},$$
$$\tilde{S}_i = \{A \in S_i : A \equiv \alpha \mod Q_i^{e_i}, \text{ for some } \alpha \in \mathbb{F}_q^\times\},$$
$$S_i^* = \{A \in S_i : A \equiv \text{a monic polynomial of degree } < \deg Q_i^{e_i} \mod Q_i^{e_i}\}.$$

For two elements A and B in S_i, we write AB to denote the element of S_i which is congruent to AB mod M. We also write A^{-1} to denote an element B of S_i such that $AB \equiv 1 \mod M$. Then every element of S can be uniquely expressed as a product of $A_1, \ldots, A_r$, where $A_i \in S_i$. Let α be a generator of $\mathbb{F}_q^\times$. We choose $\tilde{A}_i \in \tilde{S}_i$ such that $\alpha \equiv \tilde{A}_i \mod Q_i^{e_i}$.

LEMMA 2.1. *Suppose that $(B, M) = 1$. Then*

$$\sum_{A \in S_i} g\left(\frac{BA}{M}\right) = g\left(\frac{B}{M/Q_i^{e_i}}\right) - g\left(\frac{C}{M/Q_i^{e_i}}\right) \in \left(\mathsf{A}^0_{M/Q_i^{e_i}}\right)^+ \tag{6}$$

for some C.

https://doi.org/10.1017/S1446788700002275 Published online by Cambridge University Press

PROOF. The same procedure as in the classical case [2] gives the result. □

Let

$$I_M = \{(A_1, \ldots, A_r) : A_i \in S_i \text{ for } i \leq r-1, \text{ and } A_r \in S_r^*\}$$

and

$$I'_M = \{(A_1, \ldots, A_r) \in I_M \text{ satisfying one of the following conditions:}$$

- $A_r \in S_r^* \setminus \{1\}$ and $A_i \in S_i \setminus \{1\}$ for $i \leq r-1$;
- when $r-l$ is odd, $A_r = \cdots = A_{l+1} = 1$, $A_l \in (S_l \setminus \{1\}) \setminus \tilde{S}_l^*$ and $A_i \in S_i \setminus \{1\}$ for $i \leq l-1$;
- when $r-l$ is even, $A_r = \cdots = A_{l+1} = 1$, $A_l \in S_l^* \setminus \{1\}$ and $A_i \in S_i \setminus \{1\}$, for $i \leq l-1$;
- $A_r = \cdots = A_1 = 1.\}$

Here $\tilde{S}_l^* = \{A \in S_l : A \equiv \tilde{A}_l B \mod M \text{ for some } B \in S_l^*\}$.

REMARK. The difference in the definition of I'_M from that in [2] arises from the fact that there are $(q-1)$ roots of unity. In fact, if $q = 3$, then $(S_l \setminus \{1\}) \setminus \tilde{S}_l^*$ is $S_l^* \setminus \{1\}$.

LEMMA 2.2. *The cardinality $|I'_M|$ of the set I'_M is as follows*:

(i) *If r is even, $|I'_M| = 1/(q-1)\prod_{i=1}^{r}(\Phi(Q_i^{e_i}) - 1) + (q-2)/(q-1)$.*
(ii) *If r is odd, $|I'_M| = 1/(q-1)\prod_{i=1}^{r}(\Phi(Q_i^{e_i}) - 1) + 1/(q-1)$.*

In either case, we have $\sum_D |I'_D| = \Phi(M)/(q-1) + 2^{r-1} - 1$, where D runs over all monic divisors of M such that $(D, M/D) = 1$ and $D \neq 1$.

PROOF. We prove the case that r is even. The case where r is odd is very similar and we leave it to the reader. Suppose that r is even and let $X_i = \Phi(Q_i^{e_i}) - 1$ for $1 \leq i \leq r$. From the definition of I'_M, we have

$$|I'_M| = \left(\frac{X_r + 1}{q-1} - 1\right)\prod_{i=1}^{r-1} X_i + \left(\frac{q-2}{q-1}(X_{r-1} + 1) - 1\right)\prod_{i=1}^{r-2} X_i + \cdots$$
$$+ \left(\frac{X_2 + 1}{q-1} - 1\right) X_1 + \left(\frac{q-2}{q-1}(X_1 + 1) - 1\right) + 1.$$

By expanding above one, we get (i). Note that there are $\binom{r}{l}$ distinct D's such that $\pi(D) = l$ for $1 \leq l \leq r$ and that

$$\Phi(M) = \prod_{i=1}^{r}(X_i + 1) = \sum_{l=1}^{r}\left(\sum_{1 \leq i_1 < \cdots < i_l \leq r} X_{i_1} \cdots X_{i_l}\right).$$

https://doi.org/10.1017/S1446788700002275 Published online by Cambridge University Press

The results in (i), (ii) and elementary calculation show that

$$\sum_D |I'_D| = \frac{\Phi(M)}{q-1} + 2^{r-1} - 1. \qquad \square$$

Let T_M be the subgroup of $(\mathsf{A}_M^\circ)^+$ generated by

$$\left\{ g\left(\frac{A_1 \cdots A_r}{M}\right) : (A_1, \ldots, A_r) \in I'_M \right\}$$

and let

$$T'_M = \prod_D T_D,$$

where D runs over all monic divisors of M such that $(D, M/D) = 1$, $D \neq 1, M$, and T_D is defined similarly to T_M.

THEOREM 2.3.

$$(\mathsf{A}_M^\circ)^+ = T_M \times T'_M = \prod_D T_D,$$

where D runs over all monic divisors of M such that $(D, M/D) = 1$ and $D \neq 1$.

REMARK. As we have shown in Lemma 2.2, $\sum_D |I'_D| = \Phi(M)/(q-1) + 2^{\pi(M)-1} - 1$, which is the minimum number of generators of $(\mathsf{A}_M^\circ)^+$. Theorem 2.3 provides a basis (minimal set of generators) of $(\mathsf{A}_M^\circ)^+$.

PROOF OF THEOREM 2.3. We use induction on r. The case $r = 1$ is trivial. Assume the theorem holds for M with $\pi(M) \leq r - 1$. We prove $g(A_1 \cdots A_r/M) \in T_M \times T'_M$ for $(A_1, \ldots, A_r) \in I_M \setminus I'_M$ case by case.

(i) If $A_l \in (S_l \setminus \{1\}) \setminus \tilde{S}_l^*$ for $r - l$ odd, or $A_l \in S_l^* \setminus \{1\}$ for $r - l$ even, then

$$g\left(\frac{A_1 \cdots A_l}{M}\right) \in T_M \times T'_M.$$

PROOF. When none of $A_i's$ is 1, $(A_1, \ldots, A_l) \in I'_M$, then $g(A_1 \cdots A_l/M) \in T_M$. Suppose exactly one of A_i is 1, say $A_t = 1$. Then by the relation (6) in Lemma 2.1,

$$\sum_{B \in S_t} g\left(\frac{A_1 \cdots A_{t-1} B A_{t+1} \cdots A_l}{M}\right) \in T'_M.$$

Since $g(A_1 \cdots A_{t-1} B A_{t+1} \cdots A_l/M) \in T_M$ for all $B \neq 1$ by the previous case, $g(A_1 \cdots A_{t-1} 1 A_{t+1} \cdots A_l/M) \in T_M \times T'_M$. Now proceed exactly the same way as in the classical case (case (i) or (ii) of the proof of [2, Theorem 1]).

https://doi.org/10.1017/S1446788700002275 Published online by Cambridge University Press

(ii) If $A_l \notin \{1, \tilde{A}_l\}$ for $r-l$ odd, or $A_l \notin \tilde{S}_l$ for $r-l$ even, then

$$g\left(\frac{A_1 \cdots A_l}{M}\right) \in T_M \times T'_M.$$

PROOF. When $l = r$, it suffices to show that for $A_r^* \in S_r^*$, $A_r^* \neq 1$

$$g\left(\frac{A_1 \cdots A_{r-1} A_r^* \tilde{A}_r^t}{M}\right) \in T_M \times T'_M.$$

But by case (i), we have

$$g\left(\frac{A_1 \cdots A_{r-1} A_r^* \tilde{A}_r^t}{M}\right) = g\left(\frac{A_1 \tilde{A}_1^{-t} \cdots A_{r-1} \tilde{A}_{r-1}^{-t} A_r^*}{M}\right) \in T_M \times T'_M.$$

When $l = r-1$, by the definition of I'_M, it suffices to show that for $A_{r-1}^* \in S_{r-1}^*$, $A_{r-1}^* \neq 1$

$$g\left(\frac{A_1 \cdots A_{r-1}^* \tilde{A}_{r-1}}{M}\right) \in T_M \times T'_M.$$

By the relation (6) in Lemma 2.1, we have

$$g\left(\frac{A_1 \cdots A_{r-1}^* \tilde{A}_{r-1}}{M}\right) + \sum_{t=1}^{q-2} g\left(\frac{A_1 \cdots A_{r-1}^* \tilde{A}_{r-1} \tilde{A}_r^t}{M}\right) + \sum_{\substack{A_r^* \in S_r^* \\ A_r^* \neq 1}} g\left(\frac{A_1 \cdots A_{r-1}^* \tilde{A}_{r-1} A_r^*}{M}\right)$$
$$+ \sum_{\substack{A_r^* \in S_r^* \\ A_r^* \neq 1}} \sum_{t=1}^{q-2} g\left(\frac{A_1 \cdots A_{r-1}^* \tilde{A}_{r-1} A_r^* \tilde{A}_r^t}{M}\right) \in T'_M.$$

Note that

$$g\left(\frac{A_1 \cdots A_{r-1}^* \tilde{A}_{r-1} \tilde{A}_r^t}{M}\right) = g\left(\frac{A_1 \tilde{A}_1^{-t} \cdots A_{r-1}^* \tilde{A}_{r-1}^{1-t}}{M}\right) \in T_M \times T'_M$$

because $\tilde{A}_{r-1}^{1-t} \neq 1, \tilde{A}_{r-1}$ for $t \neq 1$ and $g(A_1 \tilde{A}_1^{-1} \cdots A_{r-1}^*/M) \in T_M \times T'_M$ for $t = 1$. All terms except $g(A_1 \cdots A_{r-1}^* \tilde{A}_{r-1}/M)$ are contained in $T_M \times T'_M$, by case (i) and the previous note, so $g(A_1 \cdots A_{r-1}^* \tilde{A}_{r-1}/M)$ is contained in $T_M \times T'_M$.

Now we assume that the assertion is true for $l+1, l+2, \ldots, r$ and we prove the case $r-l$ is odd. The case $r-l$ is even is very similar and we leave it to the reader. It is enough to show that for $A_l^* \in S_l^*$ and $A_l^* \neq 1$

$$g\left(\frac{A_1 \cdots A_l^* \tilde{A}_l}{M}\right) \in T_M \times T'_M. \tag{7}$$

https://doi.org/10.1017/S1446788700002275 Published online by Cambridge University Press

By the relation (6) in Lemma 2.1, we have

$$g\left(\frac{A_1\cdots A_l^*\tilde{A}_l}{M}\right)+\sum_{\alpha_{l+1}=1}^{q-2} g\left(\frac{A_1\cdots A_l^*\tilde{A}_l\tilde{A}_{l+1}^{\alpha_{l+1}}}{M}\right)+\sum_{\substack{A_{l+1}^*\in S_{l+1}^*\\ A_{l+1}^*\neq 1}} g\left(\frac{A_1\cdots A_l^*\tilde{A}_l A_{l+1}^*}{M}\right)$$
$$+\sum_{\substack{A_{l+1}^*\in S_{l+1}^*\\ A_{l+1}^*\neq 1}}\sum_{\alpha_{l+1}=1}^{q-2} g\left(\frac{A_1\cdots A_l^*\tilde{A}_l A_{l+1}^*\tilde{A}_{l+1}^{\alpha_{l+1}}}{M}\right)\in T_M'.$$

Note that the last two sums are contained in $T_M\times T_M'$ by case (i) and the inductive hypothesis. Hence (7) is equivalent to

$$\sum_{\alpha_{l+1}=1}^{q-2} g\left(\frac{A_1\cdots A_l^*\tilde{A}_l\tilde{A}_{l+1}^{\alpha_{l+1}}}{M}\right)\in T_M\times T_M'.$$

Apply the relation (6) in Lemma 2.1 again, we have

$$g\left(\frac{A_1\cdots A_l^*\tilde{A}_l\tilde{A}_{l+1}^{\alpha_{l+1}}}{M}\right)+\sum_{\alpha_{l+2}=1}^{q-2} g\left(\frac{A_1\cdots A_l^*\tilde{A}_l\tilde{A}_{l+1}^{\alpha_{l+1}}\tilde{A}_{l+2}^{\alpha_{l+2}}}{M}\right)$$
$$+\sum_{\substack{A_{l+2}^*\in S_{l+2}^*\\ A_{l+2}^*\neq 1}} g\left(\frac{A_1\cdots A_l^*\tilde{A}_l\tilde{A}_{l+1}^{\alpha_{l+1}}A_{l+2}^*}{M}\right)$$
$$+\sum_{\substack{A_{l+2}^*\in S_{l+2}^*\\ A_{l+2}^*\neq 1}}\sum_{\alpha_{l+2}=1}^{q-2} g\left(\frac{A_1\cdots A_l^*\tilde{A}_l\tilde{A}_{l+1}^{\alpha_{l+1}}A_{l+2}^*\tilde{A}_{l+2}^{\alpha_{l+2}}}{M}\right)\in T_M'.$$

The last two sums are contained in $T_M\times T_M'$ by case (i) and the inductive hypothesis and

$$g\left(\frac{A_1\cdots A_l^*\tilde{A}_l\tilde{A}_{l+1}^{\alpha_{l+1}}\tilde{A}_{l+2}^{\alpha_{l+2}}}{M}\right)\in T_M\times T_M'$$

for all $\alpha_{l+2}\neq 1$ by the inductive hypothesis (note that $r-(l+2)$ is odd). Hence

$$\sum_{\alpha_{l+1}=1}^{q-2} g\left(\frac{A_1\cdots A_l^*\tilde{A}_l\tilde{A}_{l+1}^{\alpha_{l+1}}}{M}\right)\in T_M\times T_M'$$

is equivalent to

$$\sum_{\alpha_{l+1}=1}^{q-2} g\left(\frac{A_1\cdots A_l^*\tilde{A}_l\tilde{A}_{l+1}^{\alpha_{l+1}}\tilde{A}_{l+2}}{M}\right)\in T_M\times T_M'.$$

https://doi.org/10.1017/S1446788700002275 Published online by Cambridge University Press

Repeating the above procedure, we see that (7) is equivalent to

$$(8)\qquad \sum_{\alpha_r=1}^{q-2}\cdots\sum_{\alpha_{l+1}=1}^{q-2} g\left(\frac{A_1\cdots A_l^*\tilde{A}_l\tilde{A}_{l+1}^{\alpha_{l+1}}\cdots\tilde{A}_{r-1}\tilde{A}_r^{\alpha_r}}{M}\right)\in T_M\times T_M'.$$

We claim that, for $1\le\alpha_i\le q-2$,

$$(9)\qquad g\left(\frac{A_1\cdots A_l^*\tilde{A}_l\tilde{A}_{l+1}^{\alpha_{l+1}}\tilde{A}_{l+1}\cdots\tilde{A}_{r-2}^{\alpha_{r-2}}\tilde{A}_{r-1}\tilde{A}_r^{\alpha_r}}{M}\right)\in T_M\times T_M'$$

if $\alpha_t\neq 1$ for some $t=l+1,\dots,r-2,r$.

PROOF OF CLAIM. When $\alpha_r\neq 1$, the left hand side of (9) is equal to

$$g\left(\frac{A_1\tilde{A}_1^{-\alpha_r}\cdots A_l^*\tilde{A}_l^{1-\alpha_r}\cdots\tilde{A}_{r-1}^{1-\alpha_r}}{M}\right)$$

which is contained in $T_M\times T_M'$, because $\tilde{A}_{r-1}^{1-\alpha_r}\neq 1,\tilde{A}_{r-1}$. Now we suppose that the assertion is true for $t+2,\dots,r-2,r$ and we show that for $\alpha_t\neq 1$,

$$(10)\qquad g\left(\frac{A_1\cdots A_l^*\tilde{A}_l\tilde{A}_{l+1}^{\alpha_{l+1}}\cdots\tilde{A}_{t-1}\tilde{A}_t^{\alpha_t}\tilde{A}_{t+1}\cdots\tilde{A}_{r-2}\tilde{A}_{r-1}\tilde{A}_r}{M}\right)\in T_M\times T_M'$$

which is equal to

$$g\left(\frac{A_1\tilde{A}_1^{-1}\cdots A_l^*\tilde{A}_{l+1}^{\alpha_{l+1}-1}\cdots\tilde{A}_{t-2}^{\alpha_{t-2}-1}\tilde{A}_t^{\alpha_t-1}}{M}\right).$$

By case (i), the inductive hypothesis of proof of case (ii) and the inductive hypothesis of the claim (using relation (6) in Lemma 2.1 repeatedly), (10) is equivalent to

$$(11)\qquad g\left(\frac{A_1\tilde{A}_1^{-1}\cdots A_l^*\tilde{A}_{l+1}^{\alpha_{l+1}-1}\cdots\tilde{A}_{t-2}^{\alpha_{t-2}-1}\tilde{A}_t^{\alpha_t-1}\tilde{A}_{t+1}\cdots\tilde{A}_{r-1}\tilde{A}_r}{M}\right)\in T_M\times T_M'.$$

Note that (11) is equal to

$$g\left(\frac{A_1\tilde{A}_1^{-2}\cdots A_l^*\tilde{A}_{l+1}^{\alpha_{l+1}-2}\cdots\tilde{A}_{t-2}^{\alpha_{t-2}-2}\tilde{A}_{t-1}^{-1}\tilde{A}_t^{\alpha_t-2}}{M}\right).$$

Repeating this procedure, we see that (10) is equivalent to

$$g\left(\frac{A_1\tilde{A}_1^{-\alpha_t}\cdots A_l^*\tilde{A}_l^{1-\alpha_t}\cdots\tilde{A}_{t-1}^{1-\alpha_t}}{M}\right)\in T_M\times T_M',$$

which is true because $\tilde{A}_{t-1}^{1-\alpha_t}\neq 1,\tilde{A}_{t-1}$ (note that $r-t$ is even and $t>l$). This proves our claim.

https://doi.org/10.1017/S1446788700002275 Published online by Cambridge University Press

Now we return to the proof of case (ii). By (9), (8) is equivalent to

$$g\left(\frac{A_1\cdots A_l^*\tilde{A}_l\tilde{A}_{l+1}\cdots\tilde{A}_{r-1}\tilde{A}_r}{M}\right)\in T_M\times T_M'.$$

But this term is equal to $g(A_1\tilde{A}^{-1}\cdots A_l^*/M)$ which is contained in $T_M\times T_M'$.

REMARK. The claim in the proof of (ii) is true under the inductive hypothesis of (ii). However, we have proven (ii) anyway, the claim is true in more general setting, that is,

$$g\left(\frac{A_1\cdots A_l\tilde{A}_{l+1}^{\alpha_{l+1}}\tilde{A}_{l+2}\cdots\tilde{A}_{r-1}\tilde{A}_r^{\alpha_r}}{M}\right)\in T_M\times T_M',$$

if $r-l$ is odd and $1\le\alpha_t\le q-2$, $\alpha_t\ne 1$ for some t and

$$g\left(\frac{A_1\cdots A_l\tilde{A}_{l+1}\tilde{A}_{l+2}^{\alpha_{l+2}}\cdots\tilde{A}_{r-1}\tilde{A}_r^{\alpha_r}}{M}\right)\in T_M\times T_M',$$

if $r-l$ is even and $1\le\alpha_t\le q-2$, $\alpha_t\ne 1$ for some t.

To prove the remaining cases, we need the following lemma.

LEMMA 2.4. *The following two statements are equivalent*:

(i) $g\big(A_1\cdots A_{l-1}(A_l\tilde{A}_l)/M\big)\in T_M\times T_M'$;

(ii) $g\big((A_1\tilde{A}_1^{-1})\cdots(A_{l-1}\tilde{A}_{l-1}^{-1})A_l/M\big)\in T_M\times T_M'$.

PROOF. We prove this lemma for the case $r-l$ odd. By the relation (6) in Lemma 2.1,

$$\sum_{B\in S_{l+1}} g\left(\frac{A_1\cdots A_l\tilde{A}_lB}{M}\right)\in T_M'.$$

Since $g(A_1\cdots A_l\tilde{A}_lB/M)\in T_M'$ for all $B\notin\tilde{S}_{l+1}$, by case (ii), we have

$$g\left(\frac{A_1\cdots A_l\tilde{A}_l}{M}\right)+\sum_{\alpha_{l+1}=1}^{q-2} g\left(\frac{A_1\cdots A_l\tilde{A}_l\tilde{A}_{l+1}^{\alpha_{l+1}}}{M}\right)\in T_M\times T_M'.$$

Hence

$$g\left(\frac{A_1\cdots A_l\tilde{A}_l}{M}\right)\in T_M\times T_M' \tag{12}$$

is equivalent to

$$\sum_{\alpha_{l+1}=1}^{q-2} g\left(\frac{A_1\cdots A_l\tilde{A}_l\tilde{A}_{l+1}^{\alpha_{l+1}}}{M}\right)\in T_M\times T_M'.$$

https://doi.org/10.1017/S1446788700002275 Published online by Cambridge University Press

We note that $r-(l+1)$ is even and use the relation (6) in Lemma 2.1 again, then we see that

$$\sum_{\alpha_{l+1}=1}^{q-2} g\left(\frac{A_1\cdots A_l\tilde{A}_l\tilde{A}_{l+1}^{\alpha_{l+1}}}{M}\right)\in T_M\times T'_M$$

is equivalent to

$$\sum_{\alpha_{l+1}=1}^{q-2} g\left(\frac{A_1\cdots A_l\tilde{A}_l\tilde{A}_{l+1}^{\alpha_{l+1}}\tilde{A}_{l+2}}{M}\right)\in T_M\times T'_M.$$

Therefore, (12) is equivalent to

$$\sum_{\alpha_{l+1}=1}^{q-2} g\left(\frac{A_1\cdots A_l\tilde{A}_l\tilde{A}_{l+1}^{\alpha_{l+1}}\tilde{A}_{l+2}}{M}\right)\in T_M\times T'_M.$$

Repeating the above procedure, we can see that

$$g\left(\frac{A_1\cdots A_l\tilde{A}_l}{M}\right)\in T_M\times T'_M$$

is equivalent to

$$\sum_{\alpha_r=1}^{q-2}\cdots\sum_{\alpha_{l+1}=1}^{q-2} g\left(\frac{A_1\cdots A_l\tilde{A}_l\tilde{A}_{l+1}^{\alpha_{l+1}}\cdots\tilde{A}_{r-1}\tilde{A}_r^{\alpha_r}}{M}\right)\in T_M\times T'_M. \tag{13}$$

By the remark above,

$$g\left(\frac{A_1\cdots A_l\tilde{A}_l\tilde{A}_{l+1}^{\alpha_{l+1}}\cdots\tilde{A}_{r-1}\tilde{A}_r^{\alpha_r}}{M}\right)\in T_M\times T'_M$$

for all $(\alpha_{l+1},\dots,\alpha_r)\neq(1,\dots,1)$. Hence (13) is equivalent to

$$g\left(\frac{A_1\cdots A_l\tilde{A}_l\tilde{A}_{l+1}\cdots\tilde{A}_{r-1}\tilde{A}_r}{M}\right)\in T_M\times T'_M.$$

But $g(A_1\cdots A_l\tilde{A}_l\tilde{A}_{l+1}\cdots\tilde{A}_{r-1}\tilde{A}_r/M)=g(A_1\tilde{A}_1^{-1}\cdots A_l/M)$, so we get the result. □

We return to the proof of Theorem 2.3.

(iii) If $(A_1,\dots,A_{r-1})\notin\tilde{S}_1\times\cdots\times\tilde{S}_{r-1}$, then

$$g\left(\frac{A_1A_2\cdots A_{r-1}}{M}\right)\in T_M\times T'_M.$$

PROOF. It suffices to show that

$$g\left(\frac{A_1\cdots A_l^*\tilde{A}_l^{t_l}\tilde{A}_{l+1}^{t_{l+1}}\cdots\tilde{A}_{r-1}^{t_{r-1}}}{M}\right)\in T_M\times T'_M$$

https://doi.org/10.1017/S1446788700002275 Published online by Cambridge University Press

for any l with $A_l^* \neq 1$. By Lemma 2.4, it is equivalent to

$$g\left(\frac{A_1\tilde{A}_1^{-t}\cdots A_l^*}{M}\right) \in T_M \times T'_M,$$

where $t = \sum_{i=l}^{r-1} t_i$. But it is true by case (i).

(iv) $g(\tilde{A}_1^{t_1}\cdots\tilde{A}_{r-1}^{t_{r-1}}/M) \in T_M \times T'_M$.

PROOF. By Lemma 2.4, it suffices to show that

$$g\left(\frac{\tilde{A}_1^{\alpha}}{M}\right) \in T_M \times T'_M, \quad \forall \alpha = 0, 1, \ldots, q-2.$$

If $q = 3$, then $g(\tilde{A}_1/M) + g(1/M) \in T_M \times T'_M$, by (ii) and Lemma 2.4. Since $g(1/M) \in T_M \times T'_M$, $g(\tilde{A}_1/M) \in T_M \times T'_M$. Now assume that $q > 3$. If r is even, then $r-1$ is odd. In this case

$$g\left(\frac{1}{M}\right) + g\left(\frac{\tilde{A}_1}{M}\right) + \sum_{\alpha=2}^{q-2} g\left(\frac{\tilde{A}_1^{\alpha}}{M}\right) \in T_M \times T'_M.$$

But $g(\tilde{A}_1^{\alpha}/M) \in T_M \times T'_M$ for $\alpha = 2, \ldots, q-1$ by (ii), $g(1/M) \in T_M \times T'_M$, so $g(\tilde{A}_1/M) \in T_M \times T'_M$. If r is odd, then $r-1$ is even. By Lemma 2.4, $g(\tilde{A}_1^{\alpha}/M) \in T_M \times T'_M$ is equivalent to $g(\tilde{A}_1^{\alpha+2}\tilde{A}_2^2/M) \in T_M \times T'_M$ which is true by (ii), since $r-2$ is odd. □

3. Basis of U_M

Let $M = Q_1^{e_1}Q_2^{e_2}\cdots Q_r^{e_r}$ be as before. To find a basis of U_M we eliminate certain generators of T_M. To be precise, let

$$I''_M = \begin{cases} I'_M - \{(1, \ldots, 1)\} & \text{if } r \text{ is odd;} \\ I'_M & \text{if } r \text{ is even.} \end{cases}$$

$$\tilde{g}\left(\frac{A}{M}\right) = \begin{cases} g(A/M) & \text{if } M \text{ is composite;} \\ g(A/Q^e) - g(1/Q^e) & \text{if } M = Q^e. \end{cases}$$

Let $\tilde{T}_M$ be the group generated by the elements $\tilde{g}(A_1\cdots A_r/M)$ with $(A_1, \ldots, A_r) \in I''_M$ and $\tilde{T}'_M = \prod_D \tilde{T}_D$, where D runs over all monic divisors of M such that $(D, M/D) = 1$, $D \neq 1, M$ and $\tilde{T}_D$ is defined similarly to $\tilde{T}_M$. Then we have

$$(\mathsf{A}_M^{\circ})^+ = G_1 \times G_2 \times G_3,$$

https://doi.org/10.1017/S1446788700002275 Published online by Cambridge University Press

where

$$G_1 = \tilde{T}_M \times \tilde{T}'_M,$$
$$G_2 = \text{ group generated by } \{g(1/Q_i^{e_i}) : 1 \le i \le r\},$$
$$G_3 = \text{ group generated by } \{g(1/Q_{i_1}^{e_{i_1}} \cdots Q_{i_l}^{e_{i_l}}) : l \ge 3, \text{ odd}\}.$$

LEMMA 3.1.

$$\sum_D |I''_D| = \frac{\Phi(M)}{q-1} - 1,$$

where D runs over all monic divisor of M such that $(D, M/D) = 1$ and $D \neq 1$.

PROOF. We only prove the case that r is even. Since the case r is odd is very similar, we leave it to the reader. When r is even, we have

$$\sum_D |I''_D| = \sum_D |I'_D| - \sum_{\substack{1 \le l \le r-1 \\ l \text{ odd}}} \binom{r}{r-l}$$

and $\sum_{\substack{1 \le l \le r-1 \\ l \text{ odd}}} \binom{r}{r-l}$ is 2^{r-1}. Hence the result follows. □

LEMMA 3.2. $(q-1)\, g(1/M) \in G_1$, *if M is a composite.*

PROOF. If r is even there is nothing to prove. So we assume r is odd. Let

$$R_0 = \sum_{A_1^* \in S_1^*} \sum_{A_2^* \in S_2^*} \cdots \sum_{A_r^* \in S_r^*} g\left(\frac{A_1^* A_2^* \cdots A_r^*}{M}\right)$$

and for each l, $1 \le l \le r$, let

$$R_l = \sum_{\substack{A_1^* \in S_1^* \\ 1 \le \alpha_1 \le q-2}} \cdots \sum_{\substack{A_l^* \in S_l^* \\ 1 \le \alpha_l \le q-2}} \sum_{A_{l+1}^* \in S_{l+1}^*} \cdots \sum_{A_r^* \in S_r^*} g\left(\frac{A_1^* \tilde{A}_1^{\alpha_1} \cdots A_l^* \tilde{A}_l^{\alpha_l} A_{l+1}^* \cdots A_r^*}{M}\right).$$

Then by Lemma 2.1, we have $R_i + R_{i+1} \in \tilde{T}'_M$ for each $i = 0, 1, \ldots, r-1$ and so $R_0 + R_r = (R_0 + R_1) - (R_1 + R_2) + \cdots + (R_{r-1} + R_r) \in \tilde{T}'_M$. If $(A_1^*, \ldots, A_r^*) \neq (1, \ldots, 1)$,

$$g\left(\frac{A_1^* A_2^* \cdots A_r^*}{M}\right) \in T_M \times T'_M$$

and if $(A_1^*, \ldots, A_r^*) \neq (1, \ldots, 1)$ or $\alpha_i \neq \alpha_j$ for some $i \neq j$,

$$g\left(\frac{A_1^* \tilde{A}_1^{\alpha_1} \cdots A_r^* \tilde{A}_r^{\alpha_r}}{M}\right) \in T_M \times T'_M.$$

https://doi.org/10.1017/S1446788700002275 Published online by Cambridge University Press

Thus $R_0 + R_r \in \tilde{T}'_M$ implies

$$g\left(\frac{1}{M}\right) + \sum_{1\le\alpha\le q-2} g\left(\frac{\tilde{A}_1^\alpha \cdots \tilde{A}_r^\alpha}{M}\right) \in T_M \times T'_M.$$

But $g(\tilde{A}_1^\alpha \cdots \tilde{A}_r^\alpha/M) = g(1/M)$, so the result follows. □

LEMMA 3.3. *The given generators of $G_1 \times G_2$ are linearly independent over $\mathbb{Z}$.*

PROOF. Almost the same proof as in [2] gives the result. □

LEMMA 3.4. *Let $r \ge 3$ odd. Then there exist a unique $R \in (\mathsf{A}_M^0)^+$ such that $R \ne 0$, $(q-1)R = 0$ and R is of the form*

$$R = g\left(\frac{1}{M}\right) + \sum_{\tilde{g}(A/M)\in G_1} \tilde{f}\left(\frac{A}{M}\right)\tilde{g}\left(\frac{A}{M}\right)$$

with $\tilde{f}(A/M) \in \mathbb{Z}$.

PROOF. Uniqueness is immediate by Lemma 3.3. We prove existence by induction on r. Suppose that $r = 3$. In this case $\mathrm{Tor}((\mathsf{A}_M^0)^+) \simeq \mathbb{Z}/(q-1)$, so there is $R \ne 0$ such that $(q-1)R = 0$. Since $(\mathsf{A}_M^0)^+ = G_1 \times G_2 \times G_3$, we may write

$$R = mg\left(\frac{1}{M}\right) + \sum_{\tilde{g}(A/M)\in G_1} \tilde{f}\left(\frac{A}{M}\right)\tilde{g}\left(\frac{A}{M}\right) + \sum_{i=1}^{3} f\left(\frac{1}{Q_i^{e_i}}\right) g\left(\frac{1}{Q_i^{e_i}}\right).$$

Since $(q-1)g(1/M) \in G_1$, we may assume $0 \le m \le q-2$. But if $m = 0$, then $(q-1)R = 0$ implies that $\tilde{f}(A/M) = f(1/Q_i^{e_i}) = 0$ by the linear independence (Lemma 3.3), which force $R = 0$. Hence we have $1 \le m \le q-2$. Now apply the map φ to R, then

$$1 = \varphi\left(g\left(\frac{1}{M}\right)\right) \times \prod \varphi\left(\tilde{g}\left(\frac{A}{M}\right)\right)^{\tilde{f}(A/M)} \times \prod \varphi\left(g\left(\frac{1}{Q_i^{e_i}}\right)\right)^{f(1/Q_i^{e_i})}$$

Since the first two terms of the right side are units, $f(1/Q_i^{e_i}) = 0$ and so we have

$$R = mg\left(\frac{1}{M}\right) + \sum_{\tilde{g}(A/M)\in G_1} \tilde{f}\left(\frac{A}{M}\right)\tilde{g}\left(\frac{A}{M}\right)$$

with $1 \le m \le q-2$.

https://doi.org/10.1017/S1446788700002275 Published online by Cambridge University Press

For any two nonzero distinct elements $R_1, R_2 \in \mathrm{Tor}((\mathsf{A}_M^0)^+)$, we write

$$R_i = m_i g\left(\frac{1}{M}\right) + \sum_{\tilde{g}(A/M)\in G_i} \tilde{f}_i\left(\frac{A}{M}\right)\tilde{g}\left(\frac{A}{M}\right)$$

with $1 \le m_i \le q-2$ as above, then we have $m_1 \ne m_2$. Otherwise,

$$0 = (q-1)(R_1 - R_2) = \sum_{\tilde{g}(A/M)\in G_1} (q-1)\left\{\tilde{f}_1\left(\frac{A}{M}\right) - \tilde{f}_2\left(\frac{A}{M}\right)\right\}\tilde{g}\left(\frac{A}{M}\right) \in G_1$$

which implies that $R_1 = R_2$.

Since we have $q-2$ nonzero torsion elements in $(\mathsf{A}_M^0)^+$, we can choose nonzero $R \in \mathrm{Tor}((\mathsf{A}_M^0)^+)$ of the desired form. Then we omit the rest of the induction step because it is exactly the same as in the classical case [2]. □

THEOREM 3.5. *$U_M = \varphi(G_1) \times \mathbb{F}_q^\times$, where $\varphi : (\mathsf{A}_M^\circ)^+ \to V_M/\mathbb{F}_q^\times$ is defined as in Section 1.*

REMARK. We have shown $\sum_D |I_D''| = \Phi(M)/(q-1) - 1$ in Lemma 3.1. Hence Theorem 3.5 provides a basis of U_M.

COROLLARY 3.6. *Suppose that M and N are monic with $(M, N) = 1$. Then*

$$U_{MN}^G = U_M,$$

where $G = \mathrm{Gal}(k(\Lambda_{MN})/k(\Lambda_M))$ and U_{MN}^G is the subgroup of U_{MN} fixed under the action of G.

Now we show that $U_{QM}^G = U_M$, where $G = \mathrm{Gal}(k(\Lambda_{QM})/k(\Lambda_M))$. When $Q \nmid M$, Corollary 3.6 proves it. So we assume that $Q|M$ and let $M = Q_1^{e_1}\cdots Q_r^{e_r}Q^e$ be the usual factorization of M with $e > 0$. Let $S^* = S_{r+1}^*$ as in Section 2 letting $M = Q_1^{e_1}\cdots Q_r^{e_r}Q^{e+1}$, $Q_{r+1} = Q$, and $K^* = \{A \in S^* : A \equiv 1 \mod Q^e\}$. Choose $T^* \subset S^*$ so that

$$S^* = \bigcup_{A\in T^*} A \cdot K^*.$$

For each monic divisor D of M such that $(D, M/D) = 1$, $(D, Q) = 1$, say $D = \prod_{i=1}^t Q_{i_i}^{e_{i_i}}$, we define $\tilde{T}_D''$ as the group generated by the elements $\tilde{g}(A_{i_1}\cdots A_{i_t}A/DQ^{e+1})$ with $A_{i_k} \in S_{i_k}\setminus\{1\}(k = 1, \ldots, t)$, $A \in S^*\setminus T^*$ and $\tilde{T}_M'' = \prod_D \tilde{T}_D''$. Then [2, Lemma 5] can be translated as follows:

https://doi.org/10.1017/S1446788700002275 Published online by Cambridge University Press

LEMMA 3.7. *For any* $A \in T^*$,

$$\sum_{B \in K^*} \tilde{g}\left(\frac{AB}{Q^{e+1}}\right) = \tilde{g}\left(\frac{A}{Q^e}\right) + \sum_{B \in K^*} \tilde{g}\left(\frac{B}{Q^{e+1}}\right).$$

Using Lemma 3.7 we can prove the following theorem.

THEOREM 3.8. $U_{QM} = \varphi\left(\tilde{T}_M \times \tilde{T}'_M \times \tilde{T}''_M\right) \times \mathbb{F}_q^\times$.

PROOF. The proof consists of verifying the following three cases:

(i) $\tilde{g}(A_{i_1}A_{i_2}\cdots A_{i_r}A/(DQ^{e+1})) \in \tilde{T}_{DQ^e} \times \tilde{T}'_{DQ^e} \times \tilde{T}''_{DQ^e}$ if $A \in S^* \setminus T^*$.

(ii) $\tilde{g}(A_{i_1}A_{i_2}\cdots A_{i_r}A/(DQ^{e+1})) \in \tilde{T}_{DQ^e} \times \tilde{T}'_{DQ^e} \times \tilde{T}''_{DQ^e}$ if $A \in T^*$, $A \neq 1$.

(iii) $\tilde{g}(A_{i_1}A_{i_2}\cdots A_{i_r}/(DQ^{e+1})) \in \tilde{T}_{DQ^e} \times \tilde{T}'_{DQ^e} \times \tilde{T}''_{DQ^e}$.

We will omit the proofs because they are very similar to those of [2, Theorem 3] as we did in the proof of Theorem 2.3. □

COROLLARY 3.9. *Let* $Q|M$. *Then* $U_{QM}^G = U_M$, *where* $G = \mathrm{Gal}(k(\Lambda_{QM})/k(\Lambda_M))$.

COROLLARY 3.10. *Let* M *and* N *be monic polynomials such that* $M|N$. *Then the natural map* $E_M/U_M \to E_N/U_N$ *is an injection.*

References

[1] S. Bae, 'Punctured distributions in function fields', preprint.
[2] R. Gold and J. Kim, 'Bases for cyclotomic units', *Compositio Math.* **71** (1989), 13–27.
[3] S. Galovich and M. Rosen, 'The class number of cyclotomic function fields', *J. Number Theory* **13** (1981), 363–375.
[4] ———, 'Units and class groups in cyclotomic function fields', *J. Number Theory* **14** (1982), 156–184.
[5] ———, 'Distributions on rational function fields', *Math. Ann.* **256** (1981), 549–560.
[6] L. Washington, *Introduction to cyclotomic fields* (Springer, New York, 1980).

Department of Mathematics
KAIST
Yu-song gu, Ku-song dong, 373-1
Taejon, 305-701
Korea
e-mail: shbae@math.kaist.ac.kr
e-mail: hyjung@mathx.kaist.ac.kr

https://doi.org/10.1017/S1446788700002275 Published online by Cambridge University Press