Bull. Korean Math. Soc. **29** (1992), No. 1, pp. 153–163

ON THE RING OF INTEGERS OF CYCLOTOMIC FUNCTION FIELDS

SUNGHAN BAE AND SANG-GEUN HAHN

0. Introduction

Carlitz module is used to study abelian extensions of $K = \mathbf{F}_q(T)$. In number theory every abelian etension of $\mathbf{Q}$ is contained in a cyclotomic field. Similarly every abelian extension of $\mathbf{F}_q(T)$ with some condition on ∞ is contained in a cyclotomic function field. Hence the study of cyclotomic functin fields in analogy with cyclotomic fields is an important subject in number theory. Much are known in this direction such as ring of integers, class groups and units ([G], [G-R]).

In this article we are concerned with the ring of integers in a cyclotomic function field. In [G], it is shown that the ring of integers is generated by a primitive root of the Carlitz module using the ramification theory and localization. Here we will give another proof, which is rather elementary and explicit, of this fact following the methods in [W].

Notations.

$K = \mathbf{F}_q(T)$
$A = \mathbf{F}_q[tirreduciblepolynomialinA$
$a(T), b(T), n(T)$: monic polynomial in A
α : a fixed generator of $\mathbf{F}_q^{\times}$.

enddemo

Received July 25, 1991. Revised July 29, 1991.

1. Cyclotomic Function Fields and Cyclotomic Polynomials

We define the Carlitz module ϕ on A by

$$\phi_T = TX + X^q.$$

It is known that the set $\Lambda_{a(T)}$ of roots of

$$\phi_{a(T)}(X) = 0$$

generate an abelian extension $K(\Lambda_{a(T)})$ of K, which we call the $a(T)$-th *cyclotomic function* field. By a *primitive $a(T)$-th root* of ϕ, we mean a root of $\phi_{a(T)}$ which generates the A-module $\Lambda_{a(T)}$. The properties of this extension are ;

PROPOSITION 1.1 ([H]).

a) $\mathrm{Gal}(K(\Lambda_{a(T)})/K) \cong (A/a(T))^\times$.
b) *Only the places dividing $a(T)$ and ∞ can ramify, and the ramification index at ∞ is $q-1$.*
c) *If $(a(T), b(T)) = (1)$, then $K(\Lambda_{a(T)})$ and $K(\Lambda_{b(T)})$ are linearly disjoint over K.*
d) *$K(\Lambda_{a(T)}) = K(\lambda_{a(T)})$ where $\lambda_{a(T)}$ is a primitive root of $\phi_{a(T)}$.*

As in the number field case we can define the $a(T)$-th cyclotomic polynomial $f_{a(T)}(X)$ by

$$f_{a(T)}(X) = \mathrm{Irr}(\lambda_{a(T)}, X, K)$$

where $\lambda_{a(T)}$ is a primitive $a(T)$-th root of ϕ. Then

$$(*) \qquad \prod_{\substack{d|a \\ d:\text{monic}}} f_d(X) = \phi_a(X).$$

PROPOSITION 1.2.

a) *Let $p(T)$ be an irreducible polynomial of degree d. Then*

$$\begin{aligned} f_{p(T)}(X) &= \frac{\phi_{p(T)}(X)}{X} \\ &= p(T) + a_1(T)X^{q-1} + \cdots + a_{d-1}(T)X^{q^{d-1}-1} + X^{q^d-1} \end{aligned}$$

and $p(T)|a_i(T)$ *for all* $1 \leq i \leq d-1$. *Also*

$$f_{p(T)^r}(X) = f_p(\phi_{p(T)^{r-1}}(X)).$$

b) $f_{p_1(T)^{r_1}\cdots p_s(T)^{r_s}}(X) = f_{p_1(T)\cdots p_s(T)}(\phi_{p_1(T)^{r_1-1}\cdots p_s(T)^{r_s-1}}(X))$
c) $f_{p(T)n(T)}(X) = f_{n(T)}(\phi_{p(T)}(X))/f_{n(T)}(X)$ *if* $p(T) \nmid n(T)$.
d) $f_n(X) = \left(\prod_{d|n}(\phi_{n/d}(X)\right)^{\mu(d)}$ *where*

$$\mu(d) = \begin{cases} 0 & \text{if } d \text{ is not square free} \\ (-1)^r & \text{if } d \text{ is a product of } r \text{ distinct primes} \\ 1 & \text{if } d = 1. \end{cases}$$

Proof. The proofs are mostly analogous to those in number theory, so we will only give the proof of a). The first statement is trivial. From $(*)$

$$\begin{aligned} \phi_{p(T)^r}(X) &= f_1(X)f_{p(T)}(X)\cdots f_{p(T)^r}(X) \\ &= \phi_{p(T)^{r-1}}(X)f_{p(T)^r}(X), \end{aligned}$$

so

$$\begin{aligned} f_{p(T)^r}(X) &= \phi_{p(T)^r}(X)/\phi_{p(T)^{r-1}}(X) \\ &= \phi_{p(T)}(\phi_{p(T)^{r-1}}(X))/\phi_{p(T)^{r-1}}(X) \\ &= f_{p(T)}(\phi_{p(T)^{r-1}}(X)). \end{aligned}$$

LEMMA 1.3. *Let* λ *be a primitive* $p(T)$*-th root of* ϕ. *Then*

$$\lambda f'_{p(T)}(\lambda) = p(T).$$

Proof. We know, from Proposition (1.2) a), that

$$f_{p(T)}(X) = p(T) + a_1X^{q-1} + \cdots + a_dX^{q^d-1}.$$

Hence

$$f'_{p(T)}(X) = -(a_1X^{q-2} + \cdots + a_dX^{q^d-2}).$$

Therefore

$$X \cdot f'_{p(T)}(X) = p(T) - f_{p(T)}(X).$$

Hence $\lambda f'_{p(T)}(\lambda) = p(T)$, since $f_{p(T)}(\lambda) = 0$.

We are going to generalize Lemma (1.3) for the power of $p(T)$. Let $U(X) = \dfrac{\phi_{p(T)^{r-1}}(X)}{X}$.

LEMMA 1.4. *Let λ be a primitive $p(T)^r$-th root of ϕ. Then*

$$\phi_{p(T)^{r-1}}(\lambda) \cdot f'_{p(T)^r}(\lambda) = p(T)^r.$$

Proof. We know from Proposition (1.2) a), that

$$\begin{aligned} f_{p(T)^r}(X) =& p(T) + a_1X^{q-1}U(X)^{q-1} + a_2X^{q^2-1}U(X)^{q^2-1} \\ &+ \cdots + a_dX^{q^d-1}U(X)^{q^d-1}, \end{aligned}$$

so

$$\begin{aligned} f'_{p(T)^r}(X) =& -(a_1X^{q-2}U(X)^{q-1} + a_2X^{q^2-2}U(X)^{q^2-1} \\ &+ \cdots + a_dX^{q^d-2}U(X)^{q^d-1}) \\ &- (a_1X^{q-1}U(X)^{q-2} + a_2X^{q^2-1}U(X)^{q^2-2} \\ &+ \cdots + a_dX^{q^d-1}U(X)^{q^d-2})U'(X). \end{aligned}$$

Then

$$\begin{aligned} \phi_{p(T)^{r-1}}(X) \cdot f'_{p(T)^r}(X) =& (p(T) - f_{p^r}(X))U(X) \\ &+ (p(T) - f_{p^r}(X))X \cdot U'(X). \end{aligned}$$

Evaluating at $X = \lambda$, we get

$$\phi_{p(T)^{r-1}}(\lambda)f'_{p(T)^r}(\lambda) = p(T)(U(\lambda) + \lambda U'(\lambda)).$$

As before, we have

$$U(X) + XU'(X) = U(0).$$

Hence

$$U(\lambda) + \lambda U'(\lambda) = U(0) = p(T)^{r-1},$$

and the result follows.

2. Ring of Integers

Our main theorem in this section is

THEOREM 2.1. *Let λ be a primitive $p(T)^r$-th root of ϕ. Then the ring of integers in $K(\lambda)$ over A is*

$$A[\lambda].$$

To show the theorem we need some lemmas.

LEMMA 2.2. *Let $a(T)$, $b(T) \in A$ be such that $(p(T), a(T)b(T)) = (1)$. Then $\dfrac{\phi_{a(T)}(\lambda)}{\phi_{b(T)}(\lambda)}$ is a unit in $A[\lambda]$.*

Proof. Same proof as in the number field case using the fact that

$$\frac{\phi_{b(T)c(T)}(\lambda)}{\phi_{b(T)}(\lambda)} = \frac{\phi_{c(T)}(\phi_{b(T)}(\lambda))}{\phi_{b(T)}(\lambda)}.$$

LEMMA 2.3. *(λ) is a prime ideal of $\mathcal{O}_{K(\lambda)}$ and*

$$(\lambda)^{\varphi(p(T)^r)} = (p(T))$$

where $\varphi(p(T)^r) = \#(A/p(T)^r)^* = q^{d(r-1)}(q^d - 1)$.

Proof.

$$\begin{aligned} f_{p(T)^r}(X) &= f_{p(T)}(\phi_{p(T)^{r-1}}(X)) \\ &= p(T) + a_1\phi_{p(T)^{r-1}}(X)^{q-1} + \cdots + a_d\phi_{p(T)^{r-1}}(X)^{q^d-1} \\ &= \prod_{\substack{(a,p)=1 \\ \deg a < dr}} (X - \phi_{a(T)}(\lambda)) \end{aligned}$$

Taking $X = 0$, we get the result, since $\phi_{p(T)^{r-1}}(0) = 0$.

LEMMA 2.4. *Let $A_1, \ldots, A_k$ be $r \times r$ matrices and $C = (c_{ij})$ be a $k \times k$ matrix. Then*

$$\det \begin{pmatrix} c_{11}A_1, & c_{12}A_1, & \ldots, & c_{1k}A_1 \\ c_{21}A_1, & c_{22}A_2, & \ldots, & c_{2k}A_2 \\ \vdots & & & \vdots \\ c_{k1}A_k, & c_{k2}A_k, & \ldots, & c_{kk}A_k \end{pmatrix} = \pm \det A_1 \cdot \det A_2 \cdots \det A_k (\det C)^r.$$

Proof.

$$\begin{pmatrix} c_{11}A_1, & c_{12}A_1, & \ldots, & c_{1k}A_1 \\ \vdots & & & \vdots \\ c_{k1}A_k, & c_{k2}A_k, & \ldots, & c_{kk}A_k \end{pmatrix} = \begin{pmatrix} A_1 & & & 0 \\ & A_2 & & \\ & & \ddots & \\ 0 & & & A_k \end{pmatrix} \begin{pmatrix} c_{11}I_r & c_{12}I_r & \ldots & c_{1k}I_r \\ \vdots & & & \vdots \\ c_{k1}I_r & \ldots & \ldots & \end{pmatrix}$$

By elementary column and raw operations

$$\begin{pmatrix} c_{11}I_r & c_{12} & \ldots \\ \vdots & & \\ c_{k1}I_r & \ldots & \ldots \end{pmatrix} \sim \begin{pmatrix} C & & & 0 \\ & C & & \\ & & \ddots & \\ 0 & & & C \end{pmatrix}.$$

Hence we get the result.

LEMMA 2.5. $$f_{p(T)^r}(X) = \prod_{\substack{(a,p(T))=1 \\ a:\text{monic} \\ \deg a < dr}} (X^{q-1} - \phi_{a(T)}(\lambda)^{q-1})$$

Proof. Clear from the fact that

$$\prod_{i=0}^{q-2}(X - \alpha^i \lambda) = X^{q-1} - \lambda^{q-1}.$$

LEMMA 2.6. *Let $a(T)$ be a monic polynomial with $(a(T), p(T)) = 1$ and $\deg a(T) < dr$. Then*

$$f'_{p(T)^r}(\phi_{a(T)}(\lambda)) = (\text{unit})\cdot(\text{power of } \lambda)\cdot \prod_{\substack{b\neq a \\ b:\text{monic} \\ (b,p(T))=1 \\ \deg b<dr}} (\phi_{a(T)}(\lambda)^{q-1} - \phi_{b(T)}(\lambda)^{q-1}).$$

Proof.

$$f_{p(T)^r}(X) = \prod_{\substack{b:\text{monic} \\ (b,p)=1 \\ \deg b<dr}} (X^{q-1} - \phi_{b(T)}(\lambda)^{q-1})$$

Hence

$$f'_{p(T)^r}(X) = \sum_{(c,p(T))=1} (X^{q-1} - \phi_{c(T)}(\lambda)^{q-1})' \cdot \prod_{b\neq c} (X^{q-1} - \phi_{b(T)}(\lambda)^{q-1}).$$

So

$$\begin{aligned} &f'_{p(T)^r}(\phi_{a(T)}(\lambda)) \\ &= (X^{q-1} - \phi_{a(T)}(\lambda)^{q-1})' \Big|_{X=\phi_{a(T)}(\lambda)} \prod_{b\neq a} (\phi_{a(T)}(\lambda)^{q-1} - \phi_{b(T)}(\lambda)^{q-1}). \end{aligned}$$

But

$$(X^{q-1} - \phi_{a(T)}(\lambda)^{q-1}) = \prod_{i=0}^{q-2} (X - \alpha^i \phi_{a(T)}(\lambda))$$

so

$$\begin{aligned} (X^{q-1} - \phi_{a(T)}(\lambda)^{q-1})' \Big|_{X=\phi_{a(T)}(\lambda)} &= \prod_{i=1}^{q-2} (\phi_{a(T)}(\lambda) - \alpha^i \phi_{a(T)}(\lambda)) \\ &= \phi_{a(T)}(\lambda)^{q-2} \cdot \prod_{i=1}^{q-2} (1 - \alpha^i) \\ &= (\text{unit}) \cdot \phi_{a(T)}(\lambda)^{q-2}. \end{aligned}$$

and $\phi_{a(T)}(\lambda) = (\text{unit}) \cdot \lambda$ by Lemma (2.2)

Proof of Theorem (2.1).
Let $c \in \mathcal{O}_{K(\lambda)}$. Then

$$c = a_0 + a_1\lambda + a_2\lambda^2 + \cdots + a_{(q^d-1)q^{d(r-1)}-1}\lambda^{(q^d-1)q^{d(r-1)}-1}, \qquad a_i \in K.$$

Following the methods given in [W], we get that a_i has no $p(T)$-factor in its denominator.

We assume that the set of monic polynomials prime to $p(T)$ and degree less that rd is well-ordered in some way. Write this set by

$$\{n_1, n_2, \ldots, n_k\}$$

where $k = q^{d(r-1)}(q^d-1)/(q-1)$. Let $\sigma_{n(T)}$ be the automorphism of $K(\lambda)$ associated to $n(T) \in (A/p(T)^r)^*$. Then

$$c^{\sigma_{n(T)}} = a_0 + a_1\phi_{n(T)}(\lambda) + a_2\phi_{n(T)}(\lambda)^2 + \cdots.$$

Let $c_{i,j} = c^{\sigma_{\alpha^i n_j(T)}}$. Then

$$\begin{pmatrix} c_{01} \\ c_{11} \\ \vdots \\ c_{q-1,1} \\ c_{0,2} \\ c_{1,2} \\ \vdots \end{pmatrix} = \begin{pmatrix} A_1,\ \phi_{n_1}(\lambda)^{q-1}A_1,\ \ldots,\ \phi_{n_1}(\lambda)^{(q-1)(k-1)}A_1 \\ A_2,\ \phi_{n_2}(\lambda)^{q-1}A_2,\ \ldots,\ \phi_{n_2}(\lambda)^{(q-1)(k-1)}A_2 \\ \vdots \qquad\qquad\qquad\qquad \vdots \\ A_k,\ \phi_{n_k}(\lambda)^{q-1}A_k,\ \ldots,\ \phi_{n_k}(\lambda)^{(q-1)(k-1)}A_k \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{(q-1)\cdot k} \end{pmatrix}$$

where

$$A_j = \begin{pmatrix} 1 & \phi_{n_j}(\lambda) & \phi_{n_j}(\lambda)^2 & \cdots & \phi_{n_j}(\lambda)^{q-2} \\ 1 & \alpha\phi_{n_j}(\lambda) & \cdots\cdots\cdots & & \alpha^{q-2}\phi_{n_j}(\lambda)^{q-2} \\ \vdots & \vdots & & & \vdots \\ 1 & \alpha^{q-2}\phi_{n_j}(\lambda) & \cdots\cdots\cdots & & \alpha^{q-2}\phi_{n_j}(\lambda)^{q-2} \end{pmatrix}.$$

Because c_{ij} and $\phi_{n_i}(\lambda)$ are algebraic integers, the denominators of a_i appear as factors of the determinant of the matrix

$$C = \begin{pmatrix} A_1, & \phi_{n_1}(\lambda)^{q-1}A_1, & \dots, & \phi_{n_1}(\lambda)^{(q-1)(k-1)}A_1 \\ A_2, & \phi_{n_2}(\lambda)^{q-1}A_2, & \dots, & \phi_{n_2}(\lambda)^{(q-1)(k-1)}A_2 \\ \vdots & & & \vdots \\ A_k, & \phi_{n_k}(\lambda)^{q-1}A_k, & \dots, & \phi_{n_k}(\lambda)^{(q-1)(k-1)}A_k \end{pmatrix}.$$

Hence it suffices to show that $\det C = (\text{unit}) \cdot (\text{power of } \lambda)$.

But

$$\det A_j = \prod_{i<\ell}(a^\ell - \alpha^i)\phi_{n_j}(\lambda) = (\text{unit}) \cdot (\text{power of } \lambda).$$

Let

$$B = \begin{pmatrix} 1 & \phi_{n_1}(\lambda)^{q-1}, & \dots, & \phi_{n_1}(\lambda)^{(q-1)(b-1)} \\ \vdots & & & \vdots \\ 1 & \phi_{n_k}(\lambda)^{q-1}, & \dots, & \phi_{n_k}(\lambda)^{(q-1)(b-1)} \end{pmatrix}.$$

Then

$$\det B = \prod_{i<\ell}(\phi_{n_\ell}(\lambda)^{q-1} - \phi_{n_i}(\lambda)^{q-1}).$$

By lemma 2.4, it suffices to show that $\det B = (\text{unit}) \cdot (\text{power of } \lambda)$, or equivalently,

$$(\det B)^2 = (\text{unit}) \cdot (\text{power of } \lambda).$$

But

$$(\det B)^2 = \pm \prod_{i\neq\ell}(\phi_{n_\ell}(\lambda)^{q-1} - \phi_{n_i}(\lambda)^{q-1}).$$

We know that

$$f_{p^r}(X) = \prod_{i=1}^{k}(X^{q-1} - \phi_{n_i}(\lambda)^{q-1}).$$

Then

$$f'_{p^r}(X) = \sum_j \left(\prod_{i \neq j} (X^{q-1} - \phi_{n_i}(\lambda)^{q-1}) \right) \cdot (X^{q-1} - \phi_{n_j}(\lambda)^{q-1})'$$
$$= -\sum_j X^{q-2} \left(\prod_{i \neq j} (X^{q-1} - \phi_{n_i}(\lambda)^{q-1}) \right).$$

Hence

$$f'_{p^r}(\phi_{n_j}(\lambda)) = -\phi_{n_j}(\lambda)^{q-2} \prod_{i \neq j} (\phi_{n_j}(\lambda)^{q-1} - \phi_{n_i}(\lambda)^{q-1}).$$

Therefore

$$(\det B)^2 = \pm \prod_{j=1}^{k} (f'_{p^r}(\phi_{n_j}(\lambda))/\phi_{n_j}(\lambda)^{q-2})$$
$$= \pm \prod_{j=1}^{k} p(T)^r / \phi_{p(T)^{r-1}}(\phi_{n_j}(\lambda)) \cdot \phi_{n_j}(\lambda)^{q-2}. \quad \text{(Lemma 1.4)}$$

It remains to show that $\phi_{p(T)^{r-1}}(\phi_{n_j}(\lambda))$ is (unit) $\cdot$ (power of λ). But $\phi_{p(T)^{r-1}}(\phi_{n_j}(\lambda))$ is a primitive $p(T)$-th root of ϕ. So

$$(\phi_{p(T)^{r-1}}(\phi_{n_j}(\lambda)))^{q-1} = (p(T)).$$

Since $(p(T))$ is totally ramified and $\phi_{p(T)^{r-1}}(\phi_{n_j}(\lambda))$ is an algebraic integer, $\phi_{p(T)^{r-1}}(\phi_{n_j}(\lambda))$ is (unit) $\cdot$ (power of λ).

Now following the general methods given in [W], we get

COROLLARY. *Let $n \in A$, λ_n a primitive $n(T)$-th root of ϕ. Then the ring of integers of $K(\lambda_n)$ over A is $A[\lambda_n]$.*

References

[G-R] S. Galovich-M. Rosen, *Units and Class Groups in Cyclotomic Function Fields*, J. Number Theory **14** (1982), 156–184.

[G] D. Goss, *The Arithmetic Theory of Function Fields II: The Cyclotomic Theory*, J. Algebra **81** (1983), 107–149.

[H] D. Hayes, *Explicit Class Fields Theory for Rational Function Fields*, Trans. AMS **189** (1974), 77–91.

[W] L. Washington, *Introduction to Cyclotomic Fields*, GTM 83, Springer Verlag, 1982.

Department of Mathematics, Korea Advanced Institute of Science and Technology, Taejon 305–701, Korea