Commun. Korean Math. Soc. **28** (2013), No. 1, pp. 25–38
http://dx.doi.org/10.4134/CKMS.2013.28.1.025

RESULTANTS OF CYCLOTOMIC POLYNOMIALS OVER $\mathbb{F}_q[T]$ AND APPLICATIONS

Sangtae Jeong

Abstract. In this paper we compute the resultants of the Carlitz cyclotomic polynomials and then we address two applications to the setting of the Carlitz module.

1. Introduction

The cyclotomic polynomials play a fundamental role in building on the cyclotomic theory. The resultant of any two cyclotomic polynomials was first calculated by E. Lehmer [10] and later by F. Diederichsen [6] and T. M. Apostol [1] independently. In particular, Apostol used the decomposition of reduced residue systems to explicitly calculate the resultants of two cyclotomic polynomials. Since Apostol's proof, L. Carlitz [5] used an auxiliary function associated with the roots of the cyclotomic polynomials to provide a slight generalization of Apostol's result. Besides this, S. Louboutin [11] gave another proof based on the fact that any rational number which is an algebraic integer is a rational integer. H. Lüneburg [12] also gave an independent proof to reprove a well known fact that the ring of algebraic integers in the cyclotomic field $\mathbb{Q}(\zeta_m)$ is $\mathbb{Z}[\zeta_m]$, where ζ_m is a primitive m-th root of unity.

By the well-known analogies between number fields and function fields, there are the Carlitz cyclotomic polynomials analogous to the classical cyclotomic polynomials. Bae [3] first calculated the resultants of Carlitz cyclotomic polynomials by adapting the proofs of Apostol [1, 2]. In this paper we give another proof of Bae's results by using the idea of Louboutin [11]. As consequences, we first show that the resultant for any two polynomials ρ_m, ρ_n arising from the Carlitz module ρ has a close relation with their p-resultant, which was first developed by Ore [13]. From this relation we deduce that the p-resultant of ρ_m, ρ_n lies in the underlying finite field. Secondly, as is modeled on the arguments of H. Lüneburg, we establish that the integral closure of $A = \mathbb{F}_q[T]$ in the

Received September 23, 2011; Revised September 6, 2012.
2010 *Mathematics Subject Classification.* Primary 11R09, 11R60, 12E10.
Key words and phrases. cyclotomic polynomials, resultants, p-resultants, Carlitz modules.
This work was supported by the National Research Foundation of Korea Grant funded by the Korean Government(NRF-2010-013-C00008).

cyclotomic function field $K(\lambda_m)$ is $A[\lambda_m]$, where λ_m is a primitive m-division point associated to the Carlitz module. Finally, we provide the function field analogue of Carlitz's result [5], which is a slight generalization of Bae's results.

2. Preliminaries

2.1. Carlitz module

Let us briefly recall the relevant portions of the Carlitz module. Let $\mathbb{F}_q$ be a finite field with q elements. Let $A = \mathbb{F}_q[T]$, $A^+ = \{\text{monic} \in A\}$, $K = \mathbb{F}_q(T)$, $K_\infty = \mathbb{F}_q((1/T))$ and C be the completion of an algebraic closure of K_∞. Let $C\{\tau\}$ be the non-commutative polynomial ring in τ over C with commutation rule $\tau c = c^q\tau (c \in C)$, identified with the ring of $\mathbb{F}_q$-linear polynomials $\{\sum_i a_i x^{q^i}\}$ through $\sum_i a_i\tau^i \mapsto \sum_i a_i x^{q^i}$. Let $\rho : A \to C\{\tau\}, a \mapsto \rho_a$ be the Carlitz module determined by $\rho_T = T\tau^0 + \tau$ and $\rho_\alpha = \alpha\tau^0$ for $\alpha \in \mathbb{F}_q$. For $m \in A^+$, let Λ_m be the module of m-division points, that is, the roots in C of $\rho_m(x) = 0$ and λ_m be a fixed primitive root of Λ_m. By the analytic theory the Carlitz module $\rho : A \to C\{\tau\}$ is equivalent to defining

$$\rho_a(e_L(z)) = e_L(az), \tag{1}$$

where $e_L(z)$ is the Carlitz exponential defined by $e_L(z) := z\prod_{0\neq\lambda\in\bar{\pi}A}(1 - z/\lambda)$ for an A-lattice $L = \bar{\pi}A$ and $\bar{\pi}$ the period of ρ. We refer the reader to [7] for details on the Carlitz module.

By Eq.(1) we see that the m-th cyclotomic polynomial $\Phi_m(x)$ is given by

$$\Phi_m(x) = \prod_a{}'(x - e_L(\frac{\bar{\pi}a}{m})) = \prod_a{}'(x - \rho_a(\lambda_m)), \tag{2}$$

where the $'$ indicates that a runs over non-zero polynomials in A of degree less than $\deg(m)$, which are relatively prime to m. As is in the classical case, it is easily seen that Φ_m is a polynomial with coefficients in A.

2.2. Euler's totient and Möbius function on A

We give analogues of Euler's totient and the Möbius function for A. To begin with, let m be a non-zero polynomial in A. We define $|m|$ to be the cardinality of the quotient ring A/mA, that is, $|m| = q^{\deg(m)}$. We also define $\phi(m)$ to be the number of a multiplicative group $(A/mA)^*$, whose representatives consist of non-zero polynomials in A of degree less than $\deg(m)$, which are relatively prime to m. We denote by S_m the set of such representatives of $(A/mA)^*$. Thus, S_m can be a summand of the product in Eq.(2). For a monic $m \in A^+$ the Möbius function μ on A is defined by

$$\mu(m) = \begin{cases} 1 & \text{if } m = 1, \\ (-1)^r & \text{if } m \text{ is square-free and } r \text{ is the number of} \\ & \text{monic prime factors of } m, \\ 0 & \text{if } m \text{ is not square-free.} \end{cases}$$

Notational convention. Throughout the paper, any element a in A means a monic element in A^+, unless otherwise specified, and the greatest common divisor (a, b) means the monic generator of the ideal generated by a and b in A. Also $[a, b]$ stands for the monic least common multiple of a and b. Whenever we use the notations $\sum_{d|m}$, $\prod_{d|m}$ and $\prod_{m=dd'}$, d runs through the monic divisors $d \in A^+$ of m.

We now have the crucial properties for ϕ and μ on A, parallel to classical results.

Proposition 2.1. (i) $\phi(P^e) = |P|^{e-1}(|P| - 1)$ *for a (monic) prime* $P \in A$ *and* $e \geq 1$.

(ii) $\phi(mn) = \phi(m)\phi(n)$ *if* $(m, n) = 1$.

(iii) *If* m *is a polynomial in* A, *then* $|m| = \sum_{d|m} \phi(d)$.

(iv) *For a monic* $m \in A$, $\rho_m = \prod_{d|m} \Phi_d$.

(v) *For* $m \in A$, $\sum_{d|m} \mu(d) = 1$ *if* m *is a non-zero constant,* $= 0$ *otherwise.*

(vi) (*Möbius inversion formula*) *Let* f, g *be functions from* A *into a field. For any non-zero* $m \in A$, *we have*

$$f(m) = \sum_{d|m} g(d) \quad \textit{if and only if} \quad g(m) = \sum_{d|m} \mu(m/d) f(d).$$

Proof. See [14] and [15]. □

Next we have the following recursion formulas for cyclotomic polynomials over A.

Proposition 2.2. *Let* P *be a monic prime in* A *and* r *and* M *be arbitrary monics in* A. *Then*

(i) $\Phi_{P^eM}(x) = \Phi_{PM}(\rho_{P^{e-1}}(x))$.

(ii) $\Phi_{P^eM}(x) = \begin{cases} \Phi_M(\rho_{P^e}(x))/\Phi_M(\rho_{P^{e-1}}(x)) & \textit{if } P \nmid M, \\ \Phi_M(\rho_{P^e}(x)) & \textit{otherwise.} \end{cases}$

(iii) $\Phi_{rM}(x) = \prod_{r=st} \Phi_M(\rho_s(x))^{\mu(t)}$ *if* $(r, M) = 1$.

Proof. See [4]. But we here sketch a proof. For parts (i) and (ii), use Proposition 2.1(iv) or check that both sides have the same zeros and degrees. Part (iii) follows from induction on the number of prime factors of r, together with part (ii). □

2.3. The resultant

We recall some of the interesting properties of resultants. Let D be a commutative ring with unity and $f(x), g(x)$ be two polynomials with coefficients in D, say

$$f(x) = \sum_{i=0}^{r} a_i x^i \quad \text{with } a_r \neq 0 \text{ and} \quad g(x) = \sum_{i=0}^{s} b_i x^i \quad \text{with } b_s \neq 0.$$

Then, the resultant $R(f, g)$ of f and g is defined by the determinant of a matrix $M(f, g)$ where $M(f, g)$ is the $r + s$ square matrix whose entries are arranged

in the usual fashion. We observe that $R(f,g)$ is a polynomial in a_i and b_j and that if f and g have coefficients in A, then $R(f,g)$ is also a polynomial in A. Hence $R(\Phi_m, \Phi_n)$ belongs to A for two cyclotomic polynomials over A.

Now we state the properties of resultants that are needed later.

Proposition 2.3. (i) *If* $f(x) = a_r \prod_{i=1}^{r}(x-\alpha_i)$ *and* $g(x) = b_s \prod_{j=1}^{s}(x-\beta_j)$, *then* $R(f,g) = a_r^s b_s^r \prod_i \prod_j (\alpha_i - \beta_j)$.

(ii) (*Multiplicative property*) $R(f,gh) = R(f,g)R(f,h)$.

(iii) (*Symmetric property*) $R(f,g) = (-1)^{rs} R(g,h)$.

(iv) (*Factorization property*) $R(f,g) = (-1)^{rs} b_s^r \prod_{j=1}^{s} f(\beta_j) = a_r^s \prod_{i=1}^{r} g(\alpha_i)$.

Proof. See [9]. □

By (i) in Proposition 2.3 we note that two polynomials f and g have a root in common if and only if $R(f,g) = 0$. In particular, for all monics $m, n \in A$, we have

$$R(\Phi_m, \Phi_n) = 0 \quad \text{if and only if} \quad m = n.$$

3. Resultants of Carlitz cyclotomic polynomials

For $m \in A^+$, let λ_m be a primitive root (or a generator) of Λ_m, the module of m-division points and $K_m = K(\lambda_m)$ be the cyclotomic function field and $\mathcal{O}_m$ be the integral closure of A in K_m. We say that two elements α and β in $\mathcal{O}_m$, are an associate when there exists a unit ε in $\mathcal{O}_m$ such that $\alpha = \varepsilon\beta$. As in classical case [11], it is well known that two monic polynomials in A which are equal up to a unit in $\mathcal{O}_m$, are identically the same. We use this fact to explicitly calculate the resultant of two Carlitz cyclotomic polynomials. To begin with, we see from Proposition 2.3(i) that the resultant $R(\Phi_m, \Phi_n)$ is rewritten as

$$\begin{aligned} R(\Phi_m, \Phi_n) &= \prod_a{}' \prod_b{}' \rho_{mb-na}(\lambda_{mn}) \\ &= \prod_a{}' \prod_b{}' \rho_{(mb-na)/(mn,mb-na)}(\lambda_{mn/(mn,mb-na)}), \end{aligned} \tag{3}$$

where a (b resp.) runs over elements in S_m (S_n resp.).

We will first show that $R(\Phi_m, \Phi_n)$ in Eq.(3) is monic in A and then that the right side of Eq.(3) equals a monic in A^+ up to a unit in $\mathcal{O}_m$. Hence, by the aforementioned fact we will derive the formula for the resultant of two Carlitz cyclotomic polynomials in Theorem 3.6.

We see that the constant terms of cyclotomic polynomials Φ_m are explicitly given as follows.

Lemma 3.1. *For a monic* $m \in A^+$ *we have*

$$\Phi_m(0) = \begin{cases} 0 & \text{if } m = 1, \\ P & \text{if } m = P^e \text{ where } P \text{ is a monic prime and } e \geq 1, \\ 1 & \text{otherwise.} \end{cases}$$

Proof. From Proposition 2.1(iv) we have $\rho_m(x)/x = \prod_{1\neq d|m} \Phi_d(x)$ for a monic $1 \neq m \in A$. Since $m = \prod_{1\neq d|m} \Phi_d(0)$, we see easily that $\Phi_m(0) = P$ if m is a power of some monic prime P in A, and that $\Phi_m(0) = 1$ otherwise. The remaining case of $m = 1$ is very straightforward. □

We now state the A-analogue of the decomposition of reduced residue systems in $\mathbb{Z}$.

Lemma 3.2. *Let m, d be (monic) polynomials in A such that $(m, d) = \delta$ for some $\delta \neq 0$. If a runs through a reduced residue system modulo m, then ad/δ runs through a reduced residue system modulo m/δ with each residue appearing exactly $\phi(m)/\phi(m/\delta)$.*

Proof. The proof goes on in the same way as [1]. □

We have the A-analogue of [1, Theorem 2], which shows that $R(\Phi_m, \Phi_n)$ in Eq.(3) is monic in A.

Theorem 3.3. *If m and n are distinct monics in A such that* $\deg(m) \geq \deg(n) > 0$, *we have*

$$R(\Phi_m, \Phi_n) = \prod_{d,P} P^{\mu(n/d)\phi(m)/\phi(P^a)},$$

where d runs through those monic divisors of n, and P through those monic primes such that $m/(m, d) = P^a$ for some $a \geq 1$, μ, ϕ are analogues of the Mobius function and the Euler totient for A, respectively.

Proof. By the relation (iv) in Proposition 2.1 and the multiplicative property (ii) in Proposition 2.3 we obtain $R(\Phi_m, \rho_n) = \prod_{d|n} R(\Phi_m, \Phi_d)$.

Since each factor in the preceding product is non-zero the Möbius inversion formula gives

$$R(\Phi_m, \Phi_n) = \prod_{d|n} R(\Phi_m, \rho_d)^{\mu(n/d)}. \tag{4}$$

By the symmetric property (iii) we have $R(\Phi_m, \rho_d) = R(\rho_d, \Phi_m)$ because $\phi(m)$ is even for odd prime characteristics. By the factorization property (iv) and Eqs.(2) and (1) we obtain

$$R(\rho_d, \Phi_m) = \prod_a{}' \rho_d(e_L(\bar{\pi}a/m) = \prod_a{}' e_L(\bar{\pi}ad/m),$$

where a runs over the elements in S_m. To rewrite the last product, we take a monic polynomial $\delta \in A$ such that $\delta = (m, d)$. Then we have $\frac{ad}{m} = \frac{ad/\delta}{m/\delta}$.

By Lemma 3.2, we deduce

$$R(\rho_d, \Phi_m) = \prod_b{}' e_L(\bar{\pi}b/m/\delta)^{\phi(m)/\phi(m/\delta)},$$

where b runs over the elements in $S_{m/\delta}$. Hence we have

$$R(\rho_d, \Phi_m) = \Phi_{m/\delta}(0)^{\phi(m)/\phi(m/\delta)}.$$

By Lemma 3.1 we now find

$$R(\rho_d, \Phi_m) = \begin{cases} P^{\phi(m)/\phi(m/\delta)} & \text{if } m/\delta \text{ is a power of a monic prime } P \text{ in } A, \\ 1 & \text{otherwise.} \end{cases}$$

Substituting this into Eq.(4) gives the result. □

Lemma 3.4. *Let λ_m be a generator of Λ_m and $a \in A$ be an element with $(a, m) = 1$. Then $\rho_a(\lambda_m)/\lambda_m$ is a unit in $\mathcal{O}_m$. Moveover, $\rho_a(\lambda_m)$ is a unit unless m is a power of a prime P in A, in which case $\rho_a(\lambda_m)^{\phi(m)}$ is associated to P in $\mathcal{O}_m$.*

Proof. The first assertion follows from [14, Proposition 12.6] and the second from $\Phi_m(0) = \prod_a{}' \rho_a(\lambda_m)$ and Lemma 3.1. □

We now employ Lemma 3.4 to determine under what conditions on m and n in A^+ there may exist a and b in Eq.(3) such that $mn/(mn, mb - na)$ is a power of some monic prime in A. Then we need to count the a's and b's in Eq.(3) for which $mn/(mn, mb - na)$ is a power of some prime in A.

To this end, we need the A-analogue of [11, Lemma 2].

Lemma 3.5. *Let m and n be distinct monics in A such that $\deg(m) \geq \deg(n) > 0$, and let $a \in S_m$ and $b \in S_n$. Then, $mn/(mn, mb - na)$ is a power of some monic prime $P \in A$ if and only if there exists an integer $r \geq 1$ such that $m = nP^r$ and N divides $P^r b - a$, where N is defined by $n = P^s N$ with $(P, N) = 1$. In that case, $mn/(mn, mb - na) = P^{r+s}$ and there are exactly $\phi(m)\phi(n)/\phi(N)$ pairs $(a, b) \in S_m \times S_n$ such that N divides $P^r b - a$.*

Proof. The proof of [11, Lemma 2] goes on in the same way. □

We are now in a position to state and prove the formulae for the resultants of two Carlitz cyclotomic polynomials. This result can already be found in [3, Proposition 2.5] with different arguments.

Theorem 3.6. (1) *If m and n are distinct monics in A such that $\deg(m) \geq \deg(n) > 0$, then we have*

$$R(\Phi_m, \Phi_n) = \begin{cases} P^{\phi(n)} & \text{if } m/n \text{ is a power of a monic prime } P \text{ in } A, \\ 1 & \text{otherwise,} \end{cases}$$

where $\phi(n)$ is the analogue in A for the Euler's totient.

(2) *Let m be a monic in A with $\deg(m) > 0$. Then*

$$R(\Phi_1, \Phi_m) = \begin{cases} P & \text{if } m \text{ is a power of a monic prime } P \text{ in } A, \\ 1 & \text{otherwise.} \end{cases}$$

Proof. Suppose that $m = nP^r$ for some monic prime P and $r \geq 1$. Then, by Lemmas 3.4 and 3.5 we see that there are exactly $\phi(m)\phi(n)/\phi(N)$ terms in Eq.(3) which are not associated to 1, each of which is associated to $\lambda_{P^{r+s}}$, so that their product is associated to P^e with $e = \phi(m)\phi(n)/\phi(N)\phi(P^{r+s}) = P^{\phi(n)}$. Thus, $R(\Phi_m, \Phi_n) = P^{\phi(n)}$ because $R(\Phi_m, \Phi_n)$ is associated to $P^{\phi(n)}$. Unless $m = nP^r$ for some monic prime P and $r \geq 1$, then Lemmas 3.4 and 3.5 imply $R(\Phi_m, \Phi_n)$ is a unit, so that $R(\Phi_m, \Phi_n) = 1$. Finally, the second assertion follows immediately from Lemma 3.1 by checking $R(\Phi_1, \Phi_m) = \Phi_m(0)$. □

We deduce two corollaries from Theorem 3.6.

For a polynomial $f \in A[x]$ and a prime P in A, we denote by $\bar{f} \in A/P[x]$ the polynomial obtained by reducing the coefficients of f modulo P.

Corollary 3.7. *If m and n are distinct monics in A such that* $\deg(m) \geq \deg(n) > 0$, *and* $(m, n) = 1$, *then* $(\Phi_m(a), \Phi_n(a)) = 1$ *for any* $a \in A$.

Proof. Suppose there exists a prime $P \in A$ such that P divides both $\Phi_m(a)$ and $\Phi_n(a)$ for some $a \in A$. Then the two reduced functions $\overline{\Phi_m}$, $\overline{\Phi_n}$ have a root $\bar{a} \in A/P$ in common. Hence $R(\overline{\Phi_m}, \overline{\Phi_n}) = 0$. Since $R(\Phi_m, \Phi_n) \equiv R(\overline{\Phi_m}, \overline{\Phi_n})$ (mod P) we have $R(\Phi_m, \Phi_n) \equiv 0$ (mod P), which contradicts Theorem 3.6. □

Corollary 3.8. *If m and n are distinct monics in A such that* $\deg(m) \geq \deg(n) > 0$, *and* $(m, n) = 1$, *then* $R(\rho_m(x)/x, \rho_n(x)/x) = 1$.

Proof. Using (iv) in Proposition 2.1 and the multiplicative property in Proposition 2.3, we have

$$R(\rho_m(x)/x, \rho_n(x)/x) = R(\prod_{d|m, d\neq 1} \Phi_d, \prod_{l|n, l\neq 1} \Phi_l) = \prod_{d|m, d\neq 1} \prod_{l|n, l\neq 1} R(\Phi_d, \Phi_l) = 1,$$

where the last equality follows from Theorem 3.6. □

4. Two applications

4.1. The *p*-resultant

We now want to apply the result in Corollary 3.8 to the p-resultant of $\mathbb{F}_q$-linear polynomials, which is first defined by O. Ore [13]. Let $f(\tau), g(\tau)$ be polynomials in $C\{\tau\}$ and $\{\omega_1, \ldots, \omega_r\}$ be a basis for the $\mathbb{F}_q$-vector space of the roots of $f(x)$ and let $\{\theta_1, \ldots, \theta_s\}$ be the same for $g(x)$. The p-resultant, $R_p(f(\tau), g(\tau))$ of $f(\tau)$ and $g(\tau)$ is then defined by

$$R_p(f(\tau), g(\tau)) = \frac{\Delta(\omega_1, \ldots, \omega_r, \theta_1, \ldots, \theta_s)}{\Delta(\omega_1, \ldots, \omega_r)\Delta(\theta_1, \ldots, \theta_s)},$$

where $\Delta(x_1, \ldots, x_l)$ is the Moore determinant as defined in [7]. It is well known in [7] that $\Delta(x_1, \ldots, x_l) \neq 0$ if and only if $x_1, \ldots, x_l$ are linearly independent over $\mathbb{F}_q$. We recall Ore's results on p-resultants.

Proposition 4.1. (i) $R_p(f(\tau), g(\tau))^{q-1} = R(f(x)/x, g(x)/x)$.

(ii) $R_p(f(\tau), g(\tau)) = \frac{\Delta(f(\theta_1),\ldots,f(\theta_s))}{\Delta(\theta_1,\ldots,\theta_s)} = (-1)^{rs}\frac{\Delta(g(\omega_1),\ldots,g(\omega_r))}{\Delta(\omega_1,\ldots,\omega_r)}$.

Proof. See [7] or [13]. □

Theorem 4.2. *If m and n are distinct monics in A such that $\deg(m) \geq \deg(n) > 0$, and $(m,n) = 1$, then $R_p(\rho_m(\tau), \rho_n(\tau))$ belongs to ${\mathbb{F}_q}^*$.*

Proof. The formula (i) in Proposition 4.1 applied to ρ_m and ρ_n gives

$$R_p(\rho_m(\tau), \rho_n(\tau))^{q-1} = R(\rho_m(x)/x, \rho_n(x)/x).$$

By Corollary 3.8 we have

$$R_p(\rho_m(\tau), \rho_n(\tau))^{q-1} = 1.$$

Hence the result follows. □

Proposition 4.3. *Let $\{\omega_1, \ldots, \omega_r\}$ and $\{\theta_1, \ldots, \theta_s\}$ be a basis for the $\mathbb{F}_q$-vector space of the roots of ρ_m and ρ_n respectively. If m and n are distinct monics in A such that $\deg(m) \geq \deg(n) > 0$, and $(m,n) = 1$, then $\{\rho_m(\theta_1), \ldots, \rho_m(\theta_s)\}$ and $\{\rho_n(\omega_1), \ldots, \rho_n(\omega_r)\}$ are a basis for the $\mathbb{F}_q$-vector space of the roots of ρ_n and ρ_m, respectively.*

Proof. It follows from Proposition 4.1 and Theorem 4.2. □

4.2. Integral closure of A in K_m

It is well known in the cyclotomic theory that the ring of algebraic integers in the cyclotomic field $\mathbb{Q}(\zeta_m)$ is $\mathbb{Z}[\zeta_m]$, where ζ_m is a primitive m-th root of unity. H. Lüneburg [12] applied the resultants of cyclotomic polynomials to reprove this fact. Motivated by his work, it is of interest to establish its function field analogue.

Lemma 4.4. *Let m and n be monics in A such that $m = nP^e$ for some monic prime P in A and $e \geq 1$ and let λ be a root of Φ_m.*

(i) *If $P \nmid n$ and if $g \in A[x]$ is such that $\Phi_m = \Phi_n^{\phi(P^e)} + Pg$, then $g(\lambda)$ is a unit in $A[\lambda]$.*

(ii) *If $P \mid n$ and if $g \in A[x]$ is such that $\Phi_m = \Phi_n^{|P^e|} + Pg$, then $g(\lambda)$ is a unit in $A[\lambda]$.*

Proof. Set $\psi(P^e) = \phi(P^e)$ if $P \nmid n$, $\psi(P^e) = |P^e|$ otherwise. Then we have $\phi(m) = \phi(n)\psi(P^e)$. By Theorem 3.6, (ii) and (iv) in Proposition 2.3 we get

$$P^{\phi(m)} = P^{\phi(n)\psi(P^e)} = R(\Phi_m, \Phi_n^{\psi(P^e)}) = \prod_{\Phi_m(\zeta)=0} \Phi_n(\zeta)^{\psi(P^e)}.$$

Now since $0 = \Phi_n(\zeta)^{\psi(P^e)} + Pg(\zeta)$, the preceding equation gives

$$P^{\phi(m)} = P^{\phi(m)} \prod_{\Phi_m(\zeta)=0} g(\zeta),$$

so that $g(\lambda)$ is indeed a unit. □

The following lemma is the A-analogue of Lemma 1.2 in [12].

Lemma 4.5. *Let F be a finite extension of $K = \mathbb{F}_q(T)$ and $\theta \in F$ be an integral element over A with $F = K(\theta)$. Let f be the minimal polynomial for θ over K and let P be a prime in A and $\mathcal{P}$ be a maximal ideal of $R = A[\theta]$ with $P \in \mathcal{P}$. Let $\eta \in A[x]$ be a monic polynomial of minimal degree for which $\eta(\theta) \in \mathcal{P}$ is such that $f = \eta h + Pg$ for some polynomials $g, h \in A[x]$. If $(\bar{\eta}, \bar{g}, \bar{h}) = 1$ over a field A/P, the localization of R at $\mathcal{P}$ is a discrete valuation ring.*

Proposition 4.6. *Let m be a monic in A and λ be a generator of Λ_m. Then $A[\lambda]$ is a Dedekind domain.*

Proof. Let P be a monic prime in A, and $\mathcal{P}$ be the maximal ideal of $A[\lambda]$ with $P \in \mathcal{P}$. Since Φ_m is the minimal polynomial of λ over A, then Φ_m divides ρ_m. The derivative of ρ_m is m, so that $\overline{\Phi_m}$ over A/P is square-free if m is not divisible by P. For the primes P with $|P| = 2$, if $m = PQ$ for a monic Q with $(Q, P) = 1$, then by Proposition 2.2(ii) we see that $\Phi_m(x) \equiv \Phi_Q(x) \pmod{P}$. Hence for these cases, we see by Lemma 4.5 that the localization L of $R = A[\lambda]$ at $\mathcal{P}$ is a discrete valuation ring. To deal with the remaining cases, let us write $m = P^e n$, with $n \in A$ a monic such that $(P, n) = 1$, where e is an integer ≥ 2 if $|P| = 2$, and an integer ≥ 1 otherwise. Then we have $\phi(P^e) \geq 2$. By Proposition 2.2(ii) we deduce for some $g \in A[x]$,

$$\Phi_m = \Phi_n^{\phi(P^e)} + Pg.$$

By Lemma 4.4 we see that $g(\lambda)$ is a unit in R. Putting $\varepsilon = -g(\lambda)^{-1}$ into the preceding equation gives

$$P = \Phi_n(\lambda)^{\phi(P^e)}\varepsilon.$$

Let η be the minimal polynomial of $\lambda + \mathcal{P}$ over $(A + \mathcal{P}R)/\mathcal{P} \simeq A/P$. Then η over A/P is a divisor of Φ_m, and hence of Φ_n. So there exist $H, G \in A[x]$ with $\Phi_n = \eta H + PG$. Then we have

$$P = (\eta(\lambda)H(\lambda) + PG(\lambda))^{\phi(P^e)}\varepsilon.$$

Thus, we have $\alpha_1, \beta_1 \in R$ with $P = \eta(\lambda)\alpha_1 + P^{\phi(P^e)}\beta_1$. By induction it follows that

$$P = \eta(\lambda)\alpha_i + P^{\phi(P^e)^i}\beta_i$$

with $\alpha_i, \beta_i \in R$ for all $i \in \mathbb{N}$. Let Q be the maximal ideal in the localized ring L of R at P. Then the only prime ideals of L are 0 and Q. It follows that $Q/\eta(\lambda)L$ is a prime ideal in $L/\eta(\lambda)L$. By Krull's theorem (see [8, Theorem 25. S 16]), $Q/\eta(\lambda)L$ is the nilradical of $L/\eta(\lambda)L$. Therefore $P^N \in \eta(\lambda)L$ for some positive integer N. Since $\phi(P^e) \geq 2$, there exists i such that $\phi(P^e)^i \geq N$. Then

$$P = \eta(\lambda)\alpha_i + P^{\phi(P^e)^i}\beta_i \in \eta(\lambda)L$$

and it follows that $Q = PL + \eta(\lambda)L = \eta(\lambda)L$. As in the proof of Lemma 1.2 in [12], this implies that L is a discrete valuation ring. Since the localization of R

at every maximal ideal is a discrete valuation ring and R is Noetherian, R is a Dedekind domain. □

Theorem 4.7. *Let $K_m = K(\lambda_m)$ be the cyclotomic function field and $\mathcal{O}_m$ be the integral closure of A in $K(\lambda_m)$. Then $\mathcal{O}_m = A[\lambda_m]$.*

Proof. Since a Dedekind domain is integrally closed, the result follows immediately from Proposition 4.6. □

We refer the reader to [14, Proposition 12.9] or [15, Theorem 12.5.10] for an alternate proof, which uses standard facts about Dedekind domains.

5. Generalization

We retain all notations from the previous sections, especially from Introduction and Section 2.

In this section we provide a slight generalization of the formulas for $R(\Phi_m, \Phi_n)$ in Theorem 3.6. We begin by defining an auxiliary function defined by, for monics $m, n \in A^+$

$$H_{m,n}(x) = \prod_{\alpha,\beta}(x - (\alpha - \beta)), \tag{5}$$

where α (β resp.) runs through the generators of Λ_m (Λ_n resp.).

By Proposition 2.3(i) we see that for $mn \neq 1$,

$$H_{m,n}(0) = R(\Phi_m, \Phi_n).$$

Now we shall define an element $k \in A^+$, denoted $k = (m, n)^*$, given by the greatest common divisor $k \in A^+$ of m and n in A^+ such that

$$(k, m/k) = 1, \quad (k, n/k) = 1. \tag{6}$$

As a simplest example, we shall have that for $k = 1$,

$$H_{m,n}(x) = \Phi_M(x)^{\phi(\delta)},$$

where $M = [m, n]$, $\delta = (m, n)$ in Theorem 5.6.

We need to go through several lemmas to prove our main Theorem 5.6.

Lemma 5.1. *The number of solutions $(x, y) \in S_{P^e} \times S_{P^e}$ of*

$$x - y \equiv a \pmod{P^e} \qquad (a \in A, P \nmid xy)$$

where P is a prime in A and $e > 1$ is equal to

$$\begin{cases} |P|^{e-1}(|P| - 2) & \text{if } P \nmid a, \\ |P|^{e-1}(|P| - 1) & \text{if } P \mid a. \end{cases}$$

Proof. It follows from the fact that the kernel of the natural map for $(A/P^e)^* \to (A/P)^*$ is a group of order $|P|^{e-1}$. See [14, Proposition 1.6] for a proof of this fact. □

Lemma 5.2. *Let $f(a,n)$ denote the number of solutions $(x,y) \in S_n \times S_n$ of*

$$x - y \equiv a \pmod{n}.$$

Then, for $(m,n) = 1$,

$$f(a,mn) = f(a,m)f(a,n).$$

Proof. It follows from the definition of $f(a,n)$ and the Chinese Remainder Theorem. □

For a monic $k \in A^+$ and its divisor r, write k and r as a canonical factorization of monic irreducible polynomials P_i in A^+ :

$$k = \prod P_i^{e_i}, \quad r = \prod P_i^{f_i}.$$

Define

$$k^* = \prod P_i^{e_i - 1}, \tag{7}$$

$$\psi(r,k) = \prod_{f_i < e_i} |P_i|^{e_i-1}(|P_i| - 1) \prod_{f_i = e_i} |P_i|^{e_i-1}(|P_i| - 2) \tag{8}$$

and for $su = k$ with $s, u \in A^+$, define

$$e(s,u,k) = \sum_{t|u} \mu(t)\psi(st,k).$$

Lemma 5.3. *Let notations be the same. Then*

(i) $\psi(1,k) = \phi(k)$.

(ii) *Let $s = \prod_i P_i^{g_i}$ be a monic divisor of k. Then*

$$e(s,u,k) = \begin{cases} 0 & \text{if } k^* \nmid s, \\ \prod_{g_i < e_i} |P_i|^{e_i-1} \prod_{g_i = e_i} |P_i|^{e_i-1}(|P_i| - 2) & \text{if } k^* \mid s. \end{cases}$$

(iii)

$$\sum_{su=k} e(s,u,k) = \phi(k).$$

Proof. The proofs follow from the definitions, especially the last two results from induction on the number of prime divisors of k. □

Lemma 5.4. *Let k be an element in A^+ and r be a divisor of k in A^+. Let α, β independently run through the generators of Λ_k. Then the generators of Λ_r occur $\psi(r,k)$ times among the subtraction $\alpha - \beta$, where $\psi(r,k)$ is given in Eq.*(8).

Proof. Let ε be a fixed generator of Λ_k and put $\alpha = \rho_x(\varepsilon), \beta = \rho_y(\varepsilon)$, where x, y run through reduced residue systems modulo k. Write $k = rs, \gamma = \alpha - \beta = \rho_{x-y}(\varepsilon)$. Then we see that γ is a generator of Λ_r if and only if

$$x - y \equiv as \pmod{k},$$

where $(a, r) = 1$. For fixed a and s, the number of solutions of this congruence is $f(as, k)$ as defined in Lemma 5.2. Then the result is immediate from Lemmas 5.1 and 5.2. □

Lemma 5.5. *Let $m, n \in A^+$ with $(m, n)^* = 1$. Let α run through the generators of Λ_m and β through the generators of Λ_n. Then $\gamma = \alpha - \beta$ runs through the generators of Λ_M $\phi(\delta)$ times, where*

$$\delta = (m, n) \in A^+, M = [m, n] = mn/\delta.$$

Proof. The proof easily reduces to the case where $m = P^e$ and $n = P^f$ for a prime $P \in A^+$, $e > f \geq 0$. Now if α is a generator of Λ_{P^e} and β is a generator of Λ_{P^f}, then it is easily seen that $\gamma = \alpha - \beta$ is a generator of Λ_{P^e} with each appearing exactly $\phi(P^f)$ times. □

We now have a slight generalization of Theorem 3.6.

Theorem 5.6. *Let $m, n \in A^+$ so that $(m, n)^* = k$ and put*

$$M = [m/k, n/k] \in A^+, \quad \delta = (m/k, n/k) \in A^+.$$

Then

$$H_{m,n}(x) = \prod_{su=k} \Phi_M(\rho_s(x))^{\phi(\delta)e(s,u,k)}, \tag{9}$$

where the product is restricted to those s that are divisible by k^* in Eq.(7) and $e(s, u, k)$ is evaluated by Lemma 5.3. In particular, if $k = 1$, then

$$H_{m,n}(x) = \Phi_M(x)^{\phi(\delta)},$$

where $M = [m, n]$, $\delta = (m, n)$.

Proof. For given $m, n \in A^+$, we define $k = (m, n)^*$ as is defined in Eq.(6). Write

$$m = km', n = kn'$$

so that

$$(m', n')^* = 1.$$

Then by Eq.(5) we have

$$\begin{aligned} H_{m,n}(x) &= \prod \{x - (\alpha(k) + \alpha(m')) + (\beta(k) + \beta(n'))\} \\ &= \prod \{x - (\alpha(k) - \beta(k)) - (\alpha(m') - \beta(n'))\}, \end{aligned}$$

where $\alpha(k), \beta(k)$ independently run through the primitive generators of Λ_k and $\alpha(m'), \beta(n')$ independently run through the primitive generators of $\Lambda_{m'}$ and $\Lambda_{n'}$, respectively. By Lemmas 5.4 and 5.5 we have

$$H_{m,n}(x) = \prod_{r|k} \prod \{x - (\gamma(r) - \alpha(M))\}^{\psi(r,k)\phi(\delta)}, \tag{10}$$

where in the inner product $\gamma(r)$ runs through the primitive generators of Λ_r, and $\alpha(M)$ runs though the generators of Λ_M, where

$$\delta = (m', n'), \quad M = [m', n'].$$

Since $(r, M) = 1$, $\gamma(r) - \alpha(M)$ runs through the generators of Λ_{rM}. Hence Eq.(10) becomes

$$H_{m,n}(x) = \prod_{r|k} (\Phi_{rM}(x))^{\psi(r,k)\phi(\delta)}.$$

Using the formula in Proposition 2.2(iii) we obtain

$$\begin{aligned} H_{m,n}(x) &= \prod_{r|k} \prod_{s|r} (\Phi_M(\rho_s(x))^{\mu(r/s)\psi(r,k)\phi(\delta)} \\ &= \prod_{s|k} \prod_{t|k/s} (\Phi_M(\rho_s(x))^{\mu(t)\psi(st,k)\phi(\delta)} \\ &= \prod_{s|k} (\Phi_M(\rho_s(x))^{\phi(\delta)\sum_{t|k/s}\mu(t)\psi(st,k)} \\ &= \prod_{su=k} (\Phi_M(\rho_s(x))^{\phi(\delta)e(s,u,k)}, \end{aligned}$$

where $e(s, u, k)$ is given by Lemma 5.3. Then the result follows immediately from Lemma 5.3. □

Finally we note that Theorem 3.6(1) is an easy corollary of Theorem 5.6.

Corollary 5.7. *If m and n are distinct monics in A such that* $\deg(m) \geq \deg(n) > 0$, *and $m = nP^e$ for some monic prime P, then $H_{m,n}(0) = P^{\phi(n)}$.*

Proof. For given $m = P^e n$ and n, put $k = (m, n)^*$, $M = [m/k, n/k]$ and $\delta = (m/k, n/k)$. Then we easily see that M is a power of P. By Eq.(9) and Lemma 5.3(iii) we have

$$H_{m,n}(0) = P^{\phi(\delta)\phi(k)} = P^{\phi(\delta k)}, \tag{11}$$

where the last equality follows from the relation $(\delta, k) = 1$. Now we first consider the case $(n, P) = 1$. Then we have $k = n$ and $\delta = 1$, so we obtain $H_{m,n}(0) = P^{\phi(n)}$ from Eq.(11). For the case where $(n, P) \neq 1$, write $n = n_0 P^f$ with $(P, n_0) = 1$. Then $k = n_0$ and $\delta = P^f$, so $\phi(\delta k) = \phi(P^f)\phi(n_0) = \phi(n)$, hence Eq.(11) gives the desired result. □

We close the paper by remarking that for $m = nP^e$ with a prime $P \in A^+$, we have $H_{m,n}(\zeta) = P^{\phi(n)}$ if ζ denotes an element of Λ_{k^*} (not necessarily a generator).

Acknowledgements. I would like to thank the anonymous referee for reading the manuscript carefully.

References

[1] T. M. Apostol, *Resultants of cyclotomic polynomials*, Proc. Amer. Math. Soc. **24** (1970), 457–462

[2] ———, *Euler's ϕ-function and separable Gauss sums*, Proc. Amer. Math. Soc. **24** (1970), 482–485.

[3] S. Bae, *The arithmetic of Carlitz polynomials*, J. Korean Math. Soc. **35** (1998), no. 2, 341–360.

[4] S. Bae and S. Hahn, *On the ring of integers of cyclotomic function fields*, Bull. Korean Math. Soc. **29** (1992), no. 1, 153–163.

[5] L. Carlitz, *A polynomial related to the cyclotomic polynomial*, Rend. Sem. Mat. Univ. Padova **47** (1972), 57–63.

[6] F. E. Diederichsen, *Uber die Ausreduktion ganzzahliger Gruppendarstellungen bei arithmetischer Äquivalenz*, Abh. Math. Sem. Hansischen Univ. **13** (1940), 357–412.

[7] D. Goss, *Basic Structures of Function Field Arithmetic*, Springer-Verlag, Berlin, Heidelberg, New York, 1996.

[8] I. Kaplansky, *Commutative Rings*, Bostom 1970.

[9] S. Lang, *Algebra*, (3rd edition), Addison-Wesley, Reading, MA, 1993.

[10] E. Lehmer, *A numerical function applied to cyclotomy*, Bull. Amer. Math. Soc. **36** (1930), no. 4, 291–298.

[11] S. Louboutin, *Resultants of cyclotomic polynomials*, Publ. Math. Debrecen **50** (1997), no. 1-2, 75–77.

[12] H. Lüneburg, *Resultanten von Kreisteilungspolynomen*, Arch. Math. (Basel) **42** (1984), no. 2, 139–144.

[13] O. Ore, *On a special class of polynomials*, Trans. Amer. Math. Soc. **35** (1933), no. 3, 559–584.

[14] M. Rosen, *Number Theory in Function Fields*, Springer-Verlag, Berlin, 2002.

[15] G. D. Villa Salvador, *Topics in the Theory of Algebraic Function Fields*, Mathematics: Theory & Applications. Birkhauser Boston, Inc., Boston, MA, 2006.

Department of Mathematics
Inha University
Incheon 402-751, Korea
E-mail address: stj@inha.ac.kr