

ON THE CARMICHAEL RINGS, CARMICHAEL IDEALS AND CARMICHAEL POLYNOMIALS

SUNGHAN BAE, SU HU, AND MIN SHA

ABSTRACT. Motivated by Carmichael numbers, we say that a finite ring R is a Carmichael ring if $a^{|R|} = a$ for any $a \in R$. We then call an ideal I of a ring R as a Carmichael ideal if R/I is a Carmichael ring, and a Carmichael element of R means it generates a Carmichael ideal. In this paper, we determine the structure of Carmichael rings and prove a generalization of Korselt's criterion for Carmichael ideals in Dedekind domains. We also study Carmichael elements of polynomial rings over finite fields (called Carmichael polynomials) by generalizing various classical results. For example, we show that there are infinitely many Carmichael polynomials but they have zero density.

1. INTRODUCTION

1.1. Background and motivation. By Fermat's Little Theorem, we know that if p is a prime number, then $a^p \equiv a \pmod{p}$ for any integer a . Thus, if $a^n \not\equiv a \pmod{n}$ for some integers $n > 0$ and a , then n must be a composite integer. A composite integer n is called a *Carmichael number* if $a^n \equiv a \pmod{n}$ for any integer $a \in \mathbb{Z}$. For example, the first ten Carmichael numbers are (see the sequence A002997 in the OEIS [18]):

561, 1105, 1729, 2465, 2821, 6601, 8911, 10585, 15841, 29341.

One can completely characterize all Carmichael numbers using Korselt's criterion.

Theorem 1.1 (Korselt's criterion). *A composite integer n is Carmichael if and only if n is square-free and $p - 1 \mid n - 1$ for any prime $p \mid n$.*

2010 *Mathematics Subject Classification.* 13A15, 11T06, 11R58, 11R60.

Key words and phrases. Carmichael order, Carmichael ring, Carmichael ideal, Carmichael polynomial, Dedekind domain, function field.

In 1953, Knödel [11] gave an upper bound for the number of Carmichael numbers up to x , which was improved by Erdős [5] later on. In 1994, Alford, Granville and Pomerance [1] proved that there exist infinitely many Carmichael numbers by providing a lower bound; see [6, 7] for some further improvements. Moreover, Wright [21] showed that there are infinitely many Carmichael numbers in each arithmetic progression a modulo d for positive integers a, d with $\gcd(a, d) = 1$; see [3, 12] for some previous results. Recently, Wright [22] proved that for some fixed integer m , there are infinitely many Carmichael numbers with exactly m prime factors; in fact, there are infinitely many such m .

Recently, Steele [19] generalized Carmichael numbers to ideals in number fields and proved a generalization of Korselt's criterion for these Carmichael ideals. He also showed that for any composite integer n , there are infinitely many abelian number fields K with discriminant relatively prime to n such that n does not generate a Carmichael ideal in K . Besides, Schettler [16] generalized Carmichael numbers to elements in a principal ideal domain.

In this paper, we want to generalize Carmichael numbers in a more general setting including the generalizations of Steele and Schettler as special cases, and then extend various classical or recent results about Carmichael numbers.

1.2. Our considerations. We first introduce Carmichael order of an element in a ring, which can be viewed as a generalization of the multiplicative order of a root of unity in a field.

Definition 1.2. Given a ring R , we define the *Carmichael order* of an element $a \in R$ to be the least integer $n > 1$ such that $a^n = a$ if it exists, and ∞ otherwise. We also define the *Carmichael order* of R to be the least integer $n > 1$ such that $a^n = a$ for any $a \in R$ if such an n exists, and ∞ otherwise.

By definition, all the idempotent elements of R are of Carmichael order 2. If R is a field, then its elements of finite Carmichael order are exactly the roots of unity in R .

We obtain a basic property of Carmichael order about its divisibility in Theorem 2.1 and determine the structure of rings of finite Carmichael order in Theorem 2.4.

We now introduce Carmichael rings.

Definition 1.3. A finite ring R is called a *Carmichael ring* if it is not a field and $a^{|R|} = a$ for any $a \in R$.

According to a classical result of Jacobson (see [10, Theorem 11]), a ring consisting of elements of finite Carmichael order is automatically a commutative ring. So, Carmichael rings are also commutative rings.

If n is a Carmichael number, then the residue class ring $\mathbb{Z}/n\mathbb{Z}$ is a Carmichael ring, and its Carmichael order is $\lambda(n) + 1$, where λ is the Carmichael function.

We determine the structure of Carmichael rings in Theorem 2.6, which can be viewed as a generalization of Korselt's criterion.

We also define Carmichael ideals of a ring.

Definition 1.4. An ideal I of a ring R is said to be a *Carmichael ideal* if R/I is a Carmichael ring. An element of R is called a *Carmichael element* if it generates a Carmichael ideal.

By definition, a Carmichael ideal of a commutative ring with identity is not a maximal ideal.

We prove a generalization of Korselt's criterion for Carmichael ideals for Dedekind domains in Theorem 3.1 and also study the Carmichael behaviour of ideals in the extensions of Dedekind domains.

We then consider Carmichael elements in polynomial rings over finite fields and in function fields in Sections 4 and 5 respectively.

Throughout the paper, let \mathbb{F}_q be the finite field of q elements, and $\mathbb{F}_q[t]$ the polynomial ring of one variable over \mathbb{F}_q . Following Definition 1.4, a polynomial g in $\mathbb{F}_q[t]$ is called a *Carmichael polynomial* if g generates a Carmichael ideal in $\mathbb{F}_q[t]$.

We remark here that Hsu [9] introduced another concept of Carmichael polynomials by using Carlitz modules, which is also a generalization of Carmichael numbers. The difference is that when analogizing " $a^n \equiv a \pmod{n}$ " for $\mathbb{F}_q[t]$, Hsu views the n in a^n as an element of the integer

ring \mathbb{Z} and a^n as “ n acts on a ”, but we view it as the cardinality of the residue class ring $\mathbb{Z}/n\mathbb{Z}$.

In this paper, we have extended various results about Carmichael numbers to Carmichael polynomials. For example, we establish the Korselt criterion for these polynomials (see Theorem 4.1), and we obtain lower and upper bounds for the number of monic Carmichael polynomials of fixed degree (see Theorems 4.5 and 4.6). Then, one can see that they have zero density.

Especially, we find two properties which do not hold for Carmichael numbers. The first one is that any square-free polynomial in $\mathbb{F}_q[t]$ is a factor of infinitely many Carmichael polynomials (see Theorem 4.2). The other is that any Carmichael polynomial g remains Carmichael in any finite Galois extension over $\mathbb{F}_q(t)$ with discriminant relatively prime to g (see Theorem 5.1).

2. CARMICHAEL ORDER AND CARMICHAEL RINGS

In this section, we study Carmichael order and determine the structure of Carmichael rings.

We begin with a basic property of Carmichael order.

Theorem 2.1. *Given a ring R , if $a \in R$ is of finite Carmichael order n , then for any integer $m > 1$, $a^m = a$ if and only if $n - 1 \mid m - 1$.*

Proof. For the necessity, we assume $a^m = a$. By definition, we have $m \geq n$. So, we can assume $m > n$ without loss of generality. Write $m = k_1n + r_1$ with $k_1 \geq 1$ and $0 \leq r_1 < n$. Then, noticing $a^n = a^m = a$, we have

$$a = a^m = a^{k_1n+r_1} = a^{k_1+r_1}.$$

By definition, we have $k_1 + r_1 \geq n$. If $k_1 + r_1 > n$, we write $k_1 + r_1 = k_2n + r_2$ with $k_2 \geq 1$ and $0 \leq r_2 < n$, then similarly we also have $a^{k_2+r_2} = a$. If $k_2 + r_2 > n$, then we proceed the above process again and again until we obtain integers k_j, r_j such that $a^{k_j+r_j} = a$ and $k_j + r_j = n$. Then, since $k_j + r_j \equiv 1 \pmod{n-1}$, we have for any $1 \leq i \leq j$,

$$k_i + r_i \equiv 1 \pmod{n-1}.$$

Thus, we obtain $m \equiv 1 \pmod{n-1}$, that is, $n-1 \mid m-1$.

We are now going to prove the sufficiency. Since $n-1 \mid m-1$, we write $m = k(n-1) + 1$ for some positive integer k . We further write $k = k_j n^j + \cdots + k_1 n + k_0$ with $j \geq 0$, $k_j \geq 1$ and $0 \leq k_i \leq n-1$ for each $0 \leq i \leq j$. Noticing $a^n = a$, we have

$$\begin{aligned}
a^m &= a^{k(n-1)+1} = a^{(k_j n^j + \cdots + k_1 n + k_0)(n-1)+1} \\
&= a^{((k_j-1)n^j + \cdots + k_1 n + k_0)n+1+n^{j+1}-(k_j n^j + \cdots + k_1 n + k_0)} \\
&= a^{((k_j-1)n^j + \cdots + k_1 n + k_0)n+1} \cdot a^{n^{j+1}-(k_j n^j + \cdots + k_1 n + k_0)} \\
&= a^{(k_j-1)n^j + \cdots + k_1 n + k_0+1} \cdot a^{n^{j+1}-(k_j n^j + \cdots + k_1 n + k_0)} \\
&= a^{n^{j+1}+1-n^j} = a^{(n-1)n^j+1} = a^{(n-1)+1} = a^n = a,
\end{aligned}$$

where we also use the inequalities: $(k_j-1)n^j + \cdots + k_1 n + k_0 + 1 \geq 1$ and $n^{j+1} - (k_j n^j + \cdots + k_1 n + k_0) \geq 1$. This completes the proof. \square

From Theorem 2.1, we know that the Carmichael order of a ring is equal to the maximum of the Carmichael orders of its elements. However, a ring R , consisting of elements having finite Carmichael order, might have infinite Carmichael order. For example, choosing R to be the algebraic closure of the finite field \mathbb{F}_q .

Corollary 2.2. *Assume that R is a ring of finite Carmichael order n . Then, for any integer $m > 1$, $a^m = a$ for any $a \in R$ if and only if $n-1 \mid m-1$.*

From Corollary 2.2, one can see that if a finite ring R is not a field, then it is a Carmichael ring if and only if it is of finite Carmichael order n for some integer $n > 1$ such that $n-1 \mid |R|-1$.

The Carmichael order of a ring also has connection with its character.

Theorem 2.3. *Assume that R is a ring of finite Carmichael order n . Then, the character of R is a square-free integer, and for each of its prime factors p , we have $p-1 \mid n-1$.*

Proof. Let c be the character of R . Since R is of finite Carmichael order n , for any integer $k \geq 1$ and any $a \in R$, we have

$$ka = (ka)^n = k^n a^n = k^n a,$$

and so $(k^n - k)a = 0$. This means that the character c is a positive integer, and $c \mid k^n - k$ for any integer $k \geq 1$. In particular, for any prime factor p of c , we have $c \mid p^n - p$. Thus, c is square-free. Moreover, for any prime factor p of c , since $p \mid k^n - k$ for any integer $k \geq 1$, we must have $p - 1 \mid n - 1$. \square

We now want to characterize rings of finite Carmichael order.

Theorem 2.4. *Let R be a ring with identity. Then, R is of finite Carmichael order n if and only if the natural homomorphism*

$$\sigma : R \rightarrow \prod_{\mathfrak{M}} R/\mathfrak{M}, \quad a \mapsto (a, \dots, a),$$

is injective, where \mathfrak{M} runs through all the maximal ideals of R , each R/\mathfrak{M} is a finite field, and $|R/\mathfrak{M}| - 1$ divides $n - 1$ (n is the smallest integer greater than 1 and satisfying this property).

Proof. For the necessity, R is of finite Carmichael order n . For $a \in R$, if $\sigma(a) = 0$, then $a \in \mathfrak{M}$ for each maximal ideal \mathfrak{M} of R . Besides, since $a^n = a$, we have $(1 - a^{n-1})a = 0$. If $1 - a^{n-1}$ is not a unit, then there exists a maximal ideal, say \mathfrak{M}_0 , such that $1 - a^{n-1} \in \mathfrak{M}_0$, and so $1 \in \mathfrak{M}_0$ (because $a \in \mathfrak{M}_0$), which leads to a contradiction. So, we must have that $1 - a^{n-1}$ is a unit, and thus $a = 0$. Hence, σ is injective. Moreover, since R/\mathfrak{M} is a field and each of its elements has finite multiplicative order (by assumption), we must have that R/\mathfrak{M} is a finite field. In addition, due to $a^n = a$ for any $a \in R/\mathfrak{M}$, we see that $|R/\mathfrak{M}| - 1$ divides $n - 1$. The minimality of n follows from Corollary 2.2.

Conversely, by assumption the ring $\prod_{\mathfrak{M}} R/\mathfrak{M}$ has Carmichael order n . Note that σ is injective. So, R is also of Carmichael order n . \square

We remark that in Theorem 2.4 since $|R/\mathfrak{M}| - 1$ divides $n - 1$, there are only finitely many distinct finite fields among all the finite fields R/\mathfrak{M} .

Corollary 2.5. *Let R be a ring with identity. If R is a ring of finite Carmichael order n , then the exponent of its unit group is equal to $n - 1$.*

Furthermore, in Theorem 2.4 if R has only finitely many maximal ideals, then by the Chinese remainder theorem σ is in fact an isomorphism. Note that a finite ring has only finitely many maximal ideals. We now can easily determine the structure of Carmichael rings following from Theorem 2.4.

Theorem 2.6. *Let R be a finite ring with identity. Then, R is a Carmichael ring if and only if*

$$R \cong \mathbb{F}_{q_1} \times \cdots \times \mathbb{F}_{q_k}$$

for some integer $k \geq 2$, and for each $1 \leq i \leq k$, \mathbb{F}_{q_i} is a finite field of q_i elements and $q_i - 1 \mid |R| - 1$ (the Carmichael order of R is the smallest integer $n > 1$ such that $q_i - 1 \mid n - 1$ for each $1 \leq i \leq k$).

The following corollary suggests that there exist rings R such that any non-trivial ideal of R is not a Carmichael ideal.

Corollary 2.7. *Let $\mathbb{F}_{q_1}, \mathbb{F}_{q_2}, \mathbb{F}_{q_3}$ be three distinct finite fields, and let $R = \mathbb{F}_{q_1} \times \mathbb{F}_{q_2} \times \mathbb{F}_{q_3}$. Then, any non-trivial ideal of R is not a Carmichael ideal.*

Proof. Note that a field has only trivial ideals, and a Carmichael ring is not a field. We only need to consider the ideals of R isomorphic to $\mathbb{F}_{q_1}, \mathbb{F}_{q_2}, \mathbb{F}_{q_3}$. So, it suffices to show that the following rings are not Carmichael rings:

$$\mathbb{F}_{q_1} \times \mathbb{F}_{q_2}, \quad \mathbb{F}_{q_1} \times \mathbb{F}_{q_3}, \quad \mathbb{F}_{q_2} \times \mathbb{F}_{q_3}.$$

For example, consider the ring $\mathbb{F}_{q_1} \times \mathbb{F}_{q_2}$, if it is a Carmichael ring, then by Theorem 2.6 we have

$$q_1 - 1 \mid q_1 q_2 - 1, \quad q_2 - 1 \mid q_1 q_2 - 1,$$

which implies $q_1 = q_2$. This contradicts with the assumption that \mathbb{F}_{q_1} and \mathbb{F}_{q_2} are two distinct finite fields. \square

3. CARMICHAEL IDEALS IN DEDEKIND DOMAINS

In this section, we consider Carmichael ideals in Dedekind domains.

Suppose that \mathcal{O}_K is a Dedekind ring, and K is the fraction field of \mathcal{O}_K . For any ideal \mathfrak{n} of \mathcal{O}_K , denote

$$N_K(\mathfrak{n}) = |\mathcal{O}_K/\mathfrak{n}|.$$

From Definition 1.4, an ideal \mathfrak{n} of \mathcal{O}_K is a Carmichael ideal if and only if \mathfrak{n} is a composite ideal, $N_K(\mathfrak{n})$ is finite, and for all α in \mathcal{O}_K , we have $\alpha^{N_K(\mathfrak{n})} \equiv \alpha \pmod{\mathfrak{n}}$.

Using Theorem 2.6, it is easy to get a necessary and sufficient condition for an ideal to be a Carmichael ideal in \mathcal{O}_K , generalizing Theorem 1.1 and also Korselt's criterion in number field case (see [19, Theorem 2.2]).

Theorem 3.1 (Korselt's criterion for Dedekind rings). *A composite ideal \mathfrak{n} is a Carmichael ideal of \mathcal{O}_K if and only if*

- (1) \mathfrak{n} is square-free,
- (2) $N_K(\mathfrak{n})$ is finite,
- (3) $N_K(\mathfrak{p}) - 1$ divides $N_K(\mathfrak{n}) - 1$ for any prime ideal $\mathfrak{p} \mid \mathfrak{n}$.

Proof. Suppose that \mathfrak{n} has the prime factorization:

$$\mathfrak{n} = \mathfrak{p}_1^{e_1} \mathfrak{p}_2^{e_2} \cdots \mathfrak{p}_s^{e_s},$$

where each \mathfrak{p}_i , $1 \leq i \leq s$, is a prime ideal of \mathcal{O}_K . By the Chinese Remainder Theorem, we have

$$\mathcal{O}_K/\mathfrak{n} = \mathcal{O}_K/\mathfrak{p}_1^{e_1} \times \mathcal{O}_K/\mathfrak{p}_2^{e_2} \times \cdots \times \mathcal{O}_K/\mathfrak{p}_s^{e_s}.$$

From Theorem 2.6, we get what we want. \square

We now consider Carmichael ideals in the extensions of Dedekind domains. By Theorem 3.1 we only need to consider square-free ideals.

Theorem 3.2. *Suppose that L is a finite separable extension over K of degree d , \mathfrak{n} is a square-free ideal of \mathcal{O}_K , and $N_K(\mathfrak{n})$ is finite. Let \mathcal{O}_L be the integral closure of \mathcal{O}_K in L . Then, $\mathfrak{n}\mathcal{O}_L$ is Carmichael in \mathcal{O}_L if and only if*

- (1) $\mathfrak{n}\mathcal{O}_L$ is a composite ideal,
- (2) \mathfrak{n} is relatively prime to the discriminant $\text{Disc}(L/K)$,

- (3) for each prime ideal $\mathfrak{p} \mid \mathfrak{n}$ and any prime ideal \mathfrak{P} of \mathcal{O}_L lying above \mathfrak{p} , we have $N_K(\mathfrak{p})^{f(\mathfrak{P})} - 1 \mid N_K(\mathfrak{n})^d - 1$, where $f(\mathfrak{P})$ is the residue class degree of \mathfrak{P} in L/K .

Proof. We first prove the necessity by using some basic properties of Dedekind domains. Since $\mathfrak{n}\mathcal{O}_L$ is Carmichael in \mathcal{O}_L , by Theorem 3.1 we have that $\mathfrak{n}\mathcal{O}_L$ is a composite and square-free ideal. That is, all the prime factors of \mathfrak{n} are unramified in L/K , which means that \mathfrak{n} is relatively prime to the discriminant $\text{Disc}(L/K)$. Besides, for each prime ideal $\mathfrak{p} \mid \mathfrak{n}$ and any prime ideal \mathfrak{P} of \mathcal{O}_L lying above \mathfrak{p} , by Theorem 3.1 we have that $N_L(\mathfrak{P}) - 1$ divides $N_L(\mathfrak{n}\mathcal{O}_L) - 1$. We complete the proof of this part by noticing $N_L(\mathfrak{P}) = N_K(\mathfrak{p})^{f(\mathfrak{P})}$ and $N_L(\mathfrak{n}\mathcal{O}_L) = N_K(\mathfrak{n})^d$.

Conversely, one can prove the sufficiency directly by using Theorem 3.1. \square

As in [19, Theorem 2.3], the following is a generalization of Fermat's Little Theorem to the case of Dedekind domains.

Corollary 3.3. *Let L be a finite Galois extension of K . Suppose that \mathfrak{p} is a non-zero prime ideal of \mathcal{O}_K , $N_K(\mathfrak{p})$ is finite, and \mathfrak{p} does not divide the discriminant $\text{Disc}(L/K)$. Then, we have*

$$\alpha^{N_L(\mathfrak{p}\mathcal{O}_L)} \equiv \alpha \pmod{\mathfrak{p}\mathcal{O}_L}$$

for all $\alpha \in \mathcal{O}_L$. That is, the ideal $\mathfrak{p}\mathcal{O}_L$ is either prime or Carmichael.

Proof. Since L is a finite Galois extension of K , for any prime ideal \mathfrak{P} of \mathcal{O}_L we have $f(\mathfrak{P}) \mid d$, where $d = [L : K]$. So, automatically we have $N_K(\mathfrak{p})^{f(\mathfrak{P})} - 1 \mid N_K(\mathfrak{p})^d - 1$ for any prime ideal \mathfrak{p} of \mathcal{O}_K lying below \mathfrak{P} . The rest follows from Theorem 3.2 and definition. \square

4. CARMICHAEL POLYNOMIALS OVER FINITE FIELDS

In this section, we study Carmichael polynomials in $\mathbb{F}_q[t]$.

A Korselt's type criterion for Carmichael polynomials follows directly from Theorem 3.1.

Theorem 4.1 (Korselt's criterion for polynomials). *A composite polynomial $g \in \mathbb{F}_q[t]$ is a Carmichael polynomial if and only if*

- (1) g is square-free,
- (2) for any irreducible factor P of g , $\deg P \mid \deg g$.

Proof. We only need to mention the second condition. When g is a Carmichael polynomial, then by Theorem 3.1, for any irreducible factor P of g we have that $q^{\deg P} - 1$ divides $q^{\deg g} - 1$, which is equivalent to $\deg P \mid \deg g$. \square

From Theorem 4.1, we know that any polynomial of prime degree greater than q is not a Carmichael polynomial. It is also easy to see that there are infinitely many Carmichael polynomials in $\mathbb{F}_q[t]$. Besides, for any integer $m \geq 2$, there are infinitely many Carmichael polynomials having exactly m irreducible monic factors; for example, one can choose polynomials having exactly m irreducible monic factors of the same degree.

In fact, we can construct Carmichael polynomials starting from any square-free polynomial. However, the analogue is not true for Carmichael numbers (because all Carmichael numbers are odd).

Theorem 4.2. *Let $u \in \mathbb{F}_q[t]$ be a square-free polynomial. Let $g, h \in \mathbb{F}_q[t]$ satisfy $g \neq 0$ and $\gcd(g, h) = 1$. Then, there are infinitely many square-free monic polynomials w whose irreducible monic factors are all congruent to h modulo g such that uw are Carmichael polynomials.*

Proof. Let m be the least common multiple of $\deg u$ and the degrees of all the irreducible factors of u . By Dirichlet's theorem on primes in arithmetic progressions in $\mathbb{F}_q[t]$ (see [15, Theorem 4.8]), we know that for any sufficiently large integer d , in the arithmetic progression h modulo g there exist $dm - \deg u - 1$ irreducible monic polynomials P_1, \dots, P_k ($k = dm - \deg u - 1$) of degree dm and an irreducible monic polynomial Q of degree $dm - \deg u$. Then, we obtain square-free polynomials $uP_1 \cdots P_k Q$ of degree $dm(dm - \deg u)$, which are Carmichael polynomials by Theorem 4.1. \square

As a consequence, we can confirm the infinitude of Carmichael polynomials in arithmetic progressions.

Corollary 4.3. *Given two polynomials $g, h \in \mathbb{F}_q[t]$ with $g \neq 0$, assume that $\gcd(g, h)$ is either equal to 1 or square-free. Then, there are infinitely many Carmichael monic polynomials congruent to h modulo g .*

Proof. By assumption and using Dirichlet's theorem on primes in arithmetic progressions in $\mathbb{F}_q[t]$, we have that for any sufficiently large integer d , there are square-free monic polynomials $u \in \mathbb{F}_q[t]$ of degree d such that $u \equiv h \pmod{g}$. Fix such a polynomial u . By Theorem 4.2, we see that there are infinitely many square-free monic polynomials w whose irreducible monic factors are all congruent to 1 modulo g such that uw are Carmichael polynomials. By construction, we have $uw \equiv h \pmod{g}$. This completes the proof. \square

We remark that in Corollary 4.3, if $\gcd(g, h) = 1$, then for any sufficiently large integer d , we can construct such Carmichael polynomials of the form P_1P_2 , where P_1, P_2 are irreducible monic polynomials of the same degree satisfying $P_1 \equiv h \pmod{g}$ and $P_2 \equiv 1 \pmod{g}$.

However, it is not true that for any composite integer n , there exist Carmichael polynomials of degree n . We can confirm this explicitly and further obtain some quantitative results.

We first make some preparations.

For any integer $n \geq 1$, let $\pi_q(n)$ be the number of monic irreducible polynomials of degree n in $\mathbb{F}_q[t]$. It is well-known that (for instance, see [15, Corollary of Proposition 2.1])

$$(4.1) \quad \pi_q(n) = \frac{1}{n} \sum_{d|n} \mu(d) q^{n/d},$$

where μ is the Möbius function. By [13, Lemma 4], we have

$$(4.2) \quad \frac{q^n}{n} - 2\frac{q^{n/2}}{n} \leq \pi_q(n) \leq \frac{q^n}{n}, \quad \pi_q(n) \geq \frac{q^n}{2n}.$$

Moreover, we have:

Lemma 4.4. *If $q \geq 4$, $\pi_q(n)$ is strictly increasing with respect to $n \geq 1$. Besides, both $\pi_2(n)$ and $\pi_3(n)$ are strictly increasing with respect to $n \geq 2$.*

Proof. If $q \geq 5$, then for any $n \geq 1$, using (4.2) we have

$$\pi_q(n) \leq \frac{q^n}{n} < \frac{q^{n+1}}{2(n+1)} \leq \pi_q(n+1).$$

If $q = 4$, we similarly have for any $n \geq 2$,

$$\pi_4(n) \leq \frac{4^n}{n} < \frac{4^{n+1}}{2(n+1)} \leq \pi_4(n+1).$$

From (4.1) we directly have $\pi_4(1) = 4$ and $\pi_4(2) = 6$, and so $\pi_4(1) < \pi_4(2)$.

If $q = 3$, we again have for any $n \geq 3$,

$$\pi_3(n) \leq \frac{3^n}{n} < \frac{3^{n+1}}{2(n+1)} \leq \pi_3(n+1).$$

Using (4.1), we get $\pi_3(1) = 3$, $\pi_3(2) = 3$ and $\pi_3(3) = 8$, and thus $\pi_3(2) < \pi_3(3)$.

If $q = 2$, using (4.2) we also have for any $n \geq 4$,

$$\pi_2(n) \leq \frac{2^n}{n} < \frac{2^{n+1}}{n+1} - 2 \frac{2^{(n+1)/2}}{n+1} \leq \pi_2(n+1).$$

From (4.1) we obtain $\pi_2(1) = 2$, $\pi_2(2) = 1$, $\pi_2(3) = 2$ and $\pi_2(4) = 3$, and so $\pi_2(2) < \pi_2(3) < \pi_2(4)$. \square

For any integer $n \geq 1$, let $C_q(n)$ be the number of Carmichael monic polynomials in $\mathbb{F}_q[t]$ of degree n . By Theorem 4.1, if n is a prime number and $n \leq q$, then considering the product of n distinct linear monic polynomials, we have

$$C_q(n) = \binom{q}{n};$$

otherwise if n is a prime and $n > q$, we have $C_q(n) = 0$.

Theorem 4.5. *Let n be a composite integer and ℓ the smallest prime factor of n . Then, $C_q(n) = 0$ if and only if $(q, n) = (2, 9)$. If $(q, n) \neq (2, 9)$, then $C_q(n) = 1$ if and only if $(q, n) = (2, 4)$; and moreover, we have*

$$C_q(n) \geq \frac{q^n}{(2n)^\ell}.$$

Proof. Since $\pi_2(1) = 2$, $\pi_2(2) = 1$ and $\pi_2(3) = 2$, by Theorem 4.1 we have $C_2(4) = 1$, $C_2(9) = 0$.

If $\pi_q(n/\ell) > \ell$, then we can choose polynomials g to be the product of ℓ distinct irreducible monic polynomials of degree n/ℓ . By Theorem 4.1, they are Carmichael polynomials. Counting these polynomials, we have

$$(4.3) \quad C_q(n) \geq \binom{\pi_q(n/\ell)}{\ell} \geq \pi_q(n/\ell) > \ell \geq 2.$$

So, it remains to find the condition when $\pi_q(n/\ell) > \ell$.

If $q \geq 3$, using (4.2) and noticing $q^m > 2m^2$ for any integer $m \geq 1$, we obtain

$$\pi_q(n/\ell) \geq \frac{q^{n/\ell}}{2n/\ell} > \frac{2(n/\ell)^2}{2n/\ell} = n/\ell \geq \ell.$$

Similarly, if $q = 2$, using (4.2) and noticing $2^m > 2m^2$ for any integer $m \geq 7$, we obtain for $n/\ell \geq 7$,

$$\pi_2(n/\ell) \geq \frac{2^{n/\ell}}{2n/\ell} > \frac{2(n/\ell)^2}{2n/\ell} = n/\ell \geq \ell.$$

If $n/\ell \leq 6$, then $\ell \leq 6$, and so $n \leq 36$. Thus, we only need to consider composite integers $n \leq 36$. There are only three cases $\ell = 2, 3$, or 5 .

If $\ell = 2$ and $n \geq 8$, by Lemma 4.4 we have $\pi_2(n/2) \geq \pi_2(4) = 3 > 2$.

If $\ell = 3$ and $n \geq 15$, by Lemma 4.4 we have $\pi_2(n/3) \geq \pi_2(5) = 6 > 3$.

Now, if $\ell = 5$, then $n \geq 25$, and we have $\pi_2(n/5) \geq \pi_2(5) = 6 > 5$.

So, it remains to consider $n = 6$ when $q = 2$. By (4.1), it is easy to see that $\pi_2(6/2) = 2$ and $C_2(6) = 5$.

Hence, $\pi_q(n/\ell) > \ell$ (and so (4.3)) holds for $q \geq 3$, or $q = 2$ and composite $n \neq 4, 6, 9$.

Collecting the above considerations, if $(q, n) \neq (2, 4), (2, 9)$, then $\pi_q(n/\ell) \geq \ell$, and so, by (4.3) we have

$$C_q(n) \geq \binom{\pi_q(n/\ell)}{\ell},$$

which, together with (4.2), implies that

$$C_q(n) \geq (\pi_q(n/\ell)/\ell)^\ell \geq q^n/(2n)^\ell.$$

This inequality also covers the case $(q, n) = (2, 4)$ since $C_2(4) = 1$. \square

Now, we want to get an upper bound for $C_q(n)$, which implies that the natural density of Carmichael polynomials is zero.

Theorem 4.6. *Let n be a composite number. Then, for any $0 < \varepsilon < 1/2$, there exists a constant $c(q, \varepsilon)$ such that if $n > c$, we have*

$$C_q(n) \leq \frac{q^n}{n^{1/2-\varepsilon}}.$$

Proof. We first arrange all the proper factors d_1, \dots, d_r of n as follows:

$$1 = d_1 < d_2 < \dots < d_r < n,$$

where r is the number of proper factors of n . We define a subset of r -tuples of non-negative integers:

$$T(n) = \{(k_1, \dots, k_r) : k_1 d_1 + \dots + k_r d_r = n, k_1 \leq q\}.$$

Note that since $d_1 = 1$, for each tuple (k_1, \dots, k_r) in $T(n)$, k_1 is fixed when k_2, \dots, k_r are all fixed.

For any Carmichael monic polynomial of degree n , by definition the degree of each of its irreducible monic factors divides n , and so it corresponds to one tuple in $T(n)$ by collecting the degrees of its irreducible factors. Conversely, every tuple (k_1, \dots, k_r) in $T(n)$ corresponds to

$$\binom{\pi_q(d_1)}{k_1} \dots \binom{\pi_q(d_r)}{k_r}$$

distinct Carmichael monic polynomials of degree n .

Hence, using (4.2) we obtain

$$\begin{aligned} C_q(n) &= \sum_{(k_1, \dots, k_r) \in T(n)} \binom{\pi_q(d_1)}{k_1} \dots \binom{\pi_q(d_r)}{k_r} \\ (4.4) \quad &\leq \sum_{(k_1, \dots, k_r) \in T(n)} \pi_q(d_1)^{k_1} \dots \pi_q(d_r)^{k_r} \\ &\leq \sum_{(k_1, \dots, k_r) \in T(n)} \frac{q^{k_1 d_1}}{d_1^{k_1}} \dots \frac{q^{k_r d_r}}{d_r^{k_r}} = q^n \sum_{(k_1, \dots, k_r) \in T(n)} \frac{1}{d_2^{k_2} \dots d_r^{k_r}}. \end{aligned}$$

So, it remains to estimate the summation

$$S(n) = \sum_{(k_1, \dots, k_r) \in T(n)} \frac{1}{d_2^{k_2} \dots d_r^{k_r}}.$$

Note that for each tuple $(k_1, \dots, k_r) \in T(n)$, we have $k_i \leq n/d_i$ for each $2 \leq i \leq r$ and

$$(4.5) \quad n - q \leq k_2 d_2 + \dots + k_r d_r \leq n.$$

Put

$$W(n) = \prod_{i=2}^r \left(1 + \frac{1}{d_i} + \frac{1}{d_i^2} + \cdots + \frac{1}{d_i^{n/d_i}}\right).$$

Clearly, $S(n)$ is a part of the summation $W(n)$ (after expanding the products). In the sequel, we estimate $S(n)$ by distinguishing the main part of $W(n)$.

To estimate $W(n)$, we first have

$$\begin{aligned} \log W(n) &< \log \prod_{i=2}^r \frac{1}{1 - 1/d_i} = - \sum_{i=2}^r \log(1 - 1/d_i) \\ &= \sum_{i=2}^r \left(\frac{1}{d_i} + \frac{1}{2d_i^2} + \frac{1}{3d_i^3} + \cdots \right) \\ &< \sum_{i=2}^r \left(\frac{1}{d_i} + \frac{1}{d_i^2} \right) \\ &\leq \frac{\sigma(n)}{n} - 1 - \frac{1}{n} + \int_1^n x^{-2} dx < \sigma(n)/n, \end{aligned}$$

where $\sigma(n)$ as usual is the sum of all the factors of n . Using a classical result of Robin [14, Théorème 2] that

$$\frac{\sigma(n)}{n} < \exp(\gamma) \log \log n + \frac{0.6483}{\log \log n}, \quad n \geq 3,$$

where γ is the Euler-Mascheroni constant ($\gamma = 0.577215664901532 \dots$), we directly have for $n \geq 268$

$$\frac{\sigma(n)}{n} < 2 \log \log n - 0.2189 \log \log n + \frac{0.6483}{\log \log n} < 2 \log \log n.$$

Hence, we obtain

$$(4.6) \quad W(n) < (\log n)^2, \quad n \geq 268.$$

Now, we want to find the main part of $W(n)$. For a fixed $0 < \varepsilon < 1/2$, let $j \geq 1$ be the unique index satisfying

$$1 = d_1 < d_2 < \cdots < d_j < (n - q)^{(1-\varepsilon)/2} \leq d_{j+1} < \cdots < d_r.$$

For each $2 \leq i \leq r$, let

$$m_i = \lfloor ((n - q)/d_i)^{2\varepsilon/(1+\varepsilon)} \rfloor.$$

Then, since

$$\begin{aligned} \sum_{i=2}^j m_i d_i &\leq (n-q)^{2\varepsilon/(1+\varepsilon)} \sum_{i=2}^j d_i^{(1-\varepsilon)/(1+\varepsilon)} \\ &< (n-q)^{2\varepsilon/(1+\varepsilon)} \int_1^{(n-q)^{(1-\varepsilon)/2}} x^{(1-\varepsilon)/(1+\varepsilon)} dx \\ &< (n-q)^{2\varepsilon/(1+\varepsilon)} \cdot (n-q)^{(1-\varepsilon)/(1+\varepsilon)} = n-q, \end{aligned}$$

in view of (4.5) we know that any summation term of

$$V(n) = \prod_{i=2}^j \left(1 + \frac{1}{d_i} + \frac{1}{d_i^2} + \cdots + \frac{1}{d_i^{m_i}}\right)$$

(after expanding the products) does not appear in $S(n)$. Thus, we have

$$(4.7) \quad S(n) \leq W(n) - V(n).$$

It suffices to estimate $W(n) - V(n)$.

For each $2 \leq i \leq j$, we have

$$(4.8) \quad \begin{aligned} \frac{1}{d_i^{m_i+1}} + \frac{1}{d_i^{m_i+2}} + \cdots + \frac{1}{d_i^{m_i/d_i}} &< \frac{1/d_i^{m_i+1}}{1-1/d_i} = \frac{1}{(d_i-1)d_i^{m_i}} \\ &\leq 2^{-m_i} \leq 2^{1-(n-q)^\varepsilon}. \end{aligned}$$

On the other hand, for each $j+1 \leq i \leq r$ we have

$$(4.9) \quad \begin{aligned} \frac{1}{d_i} + \frac{1}{d_i^2} + \cdots + \frac{1}{d_i^{m_i/d_i}} &< \frac{1/d_i}{1-1/d_i} = \frac{1}{d_i-1} \\ &\leq \frac{1}{(n-q)^{(1-\varepsilon)/2} - 1}. \end{aligned}$$

Therefore, combining (4.8), (4.9) with (4.6), we deduce that

$$(4.10) \quad \begin{aligned} W(n) - V(n) &\leq \sum_{i=2}^j \left(\frac{1}{d_i^{m_i+1}} + \frac{1}{d_i^{m_i+2}} + \cdots + \frac{1}{d_i^{m_i/d_i}} \right) W(n) \\ &\quad + \sum_{i=j+1}^r \left(\frac{1}{d_i} + \frac{1}{d_i^2} + \cdots + \frac{1}{d_i^{m_i/d_i}} \right) W(n) \\ &\leq \left(2^{1-(n-q)^\varepsilon} + ((n-q)^{(1-\varepsilon)/2} - 1)^{-1} \right) (\log n)^2 \tau(n), \end{aligned}$$

where $\tau(n)$ is the number of factors of n . For $\tau(n)$, a classical result of Wigert says that (see, for instance, [2, Theorem 13.12])

$$\tau(n) = n^{O(1/\log \log n)}.$$

Hence, for sufficiently large n (depending on q, ε), (4.10) becomes

$$(4.11) \quad W(n) - V(n) \leq n^{-1/2+\varepsilon}.$$

Finally, the desired result follows from (4.4), (4.7) and (4.11). \square

Corollary 4.7. *The natural density of Carmichael monic polynomials in $\mathbb{F}_q[t]$ is zero. That is, we have*

$$\lim_{n \rightarrow \infty} \frac{C_q(1) + C_q(2) + \cdots + C_q(n)}{q^n} = 0.$$

Finally, we extend the concept of Carmichael polynomials as the integer case.

Recall that for any integer $d \geq 1$, a *rigid Carmichael number of order d* is a composite square-free integer n satisfying $p^i - 1 \mid n^d - 1$ for all primes $p \mid n$ and all $1 \leq i \leq d$ (see [8] or the comments after Theorem 2.7 in [19]). It is conjectured that there are infinitely many rigid Carmichael numbers of order d for any $d \geq 2$.

Similarly, we define a *rigid Carmichael polynomial of order d* in $\mathbb{F}_q[t]$ to be a reducible square-free polynomial $g \in \mathbb{F}_q[t]$ satisfying $i \deg P \mid d \deg g$ for any irreducible polynomial P dividing g and any $i = 1, \dots, d$. For example, let $g = P_1 P_2$ with $\deg P_i = 3$ and $d = 3$, then g is a Carmichael polynomial of order 3 in $\mathbb{F}_q[t]$.

Theorem 4.8. *For any positive integer d , there exist infinitely many rigid Carmichael monic polynomials of order d in $\mathbb{F}_q[t]$.*

Proof. We only need to consider the case when $d \geq 2$. Fix a positive integer $d \geq 2$. Let m be the least common multiple of $1, 2, \dots, d$. For any positive integer n satisfying $\pi_q(n) \geq m$, we can construct polynomials $g = P_1 \cdots P_m$, where P_1, \dots, P_m are distinct monic irreducible polynomials of degree n . Then, $\deg g = mn$. Thus, for any $1 \leq j \leq m$ and $1 \leq i \leq d$, we have $i \deg P_j = in \mid d \deg g = dmn$, and so g is a rigid Carmichael polynomial of order d . Letting n go to ∞ , we get infinity many such polynomials g . This completes the proof. \square

5. CARMICHAEL ELEMENTS IN FUNCTION FIELDS

Let K be a function field (that is, a finite extension over $\mathbb{F}_q(t)$), and let \mathcal{O}_K be the ring of integers of K . We say that an element $\alpha \in \mathcal{O}_K$ is Carmichael in K if α is a Carmichael element of \mathcal{O}_K (see Definition 1.4).

In this section, as the number field case [19], we consider the following questions:

- (1) For any function field K , does it have infinitely many Carmichael elements?
- (2) For any square-free polynomial g in $\mathbb{F}_q[t]$, is it Carmichael in infinitely many function fields with discriminant relatively prime to g ?
- (3) For any square-free polynomial g in $\mathbb{F}_q[t]$, is it not Carmichael in infinitely many function fields with discriminant relatively prime to g ?

We give a definite answer to the first question (see Corollary 5.4 below) and some partial answers to the second and third questions whose answers we conjecture are both positive.

First, we consider the case of Carmichael polynomials in $\mathbb{F}_q[t]$.

Theorem 5.1. *Let g be a Carmichael polynomial in $\mathbb{F}_q[t]$. Then, g is Carmichael in any finite Galois extension over $\mathbb{F}_q(t)$ with discriminant relatively prime to g .*

Proof. Suppose that K is a finite Galois extension over $\mathbb{F}_q(t)$ with degree d and discriminant $\text{Disc}(K)$. For any irreducible factor P of g , let $f(P)$ be the residue class degree of P in $K/\mathbb{F}_q(t)$. Due to the choice of K , we have $f(P) \mid d$. Since g is relatively prime to $\text{Disc}(K)$, each irreducible factor of g is unramified in $K/\mathbb{F}_q(t)$. Note that g is a Carmichael polynomial in $\mathbb{F}_q[t]$. Then, the ideal $g\mathcal{O}_K$ is square-free, and for any irreducible factor P of g , we have $\deg P \mid \deg g$. Given a prime ideal \mathfrak{p} of K lying above P , we have

$$N_K(\mathfrak{p}) = N_{\mathbb{F}_q(t)}(P)^{f(P)} = q^{f(P)\deg P}.$$

Then, noticing $N_K(g\mathcal{O}_K) = q^{d\deg g}$ and $f(P)\deg P \mid d\deg g$, we have

$$N_K(\mathfrak{p}) - 1 \mid N_K(g\mathcal{O}_K) - 1.$$

Hence, from Theorem 3.1, g is Carmichael in K . \square

We remark that the number field case does not have a similar result as the above theorem; see [19, Theorem 3.1].

However, a Carmichael polynomial might not be Carmichael in infinitely many function fields. More generally, we have:

Theorem 5.2. *Let g be a square-free polynomial in $\mathbb{F}_q[t]$ of odd degree. Assume that $3 \nmid q$ and $3 \nmid q-1$. Then, g is not Carmichael in infinitely many cubic function fields over $\mathbb{F}_q(t)$ with discriminant relatively prime to g .*

Proof. By assumption, we can choose an irreducible factor, say P , of g such that the degree $\deg P$ is odd. Noticing that $3 \nmid q$ and $3 \nmid q-1$, we have $3 \mid q^{\deg P} + 1$. We choose two distinct irreducible polynomials $G, H \in \mathbb{F}_q[t]$ not dividing g such that

$$G \equiv H \pmod{P}.$$

Let $D = GH^2$. So, D is a cube modulo P . Let K be the cubic function field generated by $\sqrt[3]{D}$, which is a cubic root of D over $\mathbb{F}_q(t)$. Then, the discriminant of $K/\mathbb{F}_q(t)$ is $-27G^2H^2$ (see [16, page 610]), which is indeed relatively prime to g . Then, by [16, Theorem 3.1], we have that $P\mathcal{O}_K$ is a product of two distinct prime ideals in \mathcal{O}_K , say \mathfrak{p}_1 and \mathfrak{p}_2 . So, for the residue class degrees $f(\mathfrak{p}_1)$ and $f(\mathfrak{p}_2)$, one of them is equal to 2, say $f(\mathfrak{p}_1)$. Clearly, $N_K(\mathfrak{p}_1) = q^{f(\mathfrak{p}_1)\deg P} = q^{2\deg P}$, and $N_K(g\mathcal{O}_K) = q^{3\deg g}$. Noticing $2 \nmid 3\deg g$, we have

$$N_K(\mathfrak{p}_1) - 1 \nmid N_K(g\mathcal{O}_K) - 1,$$

which implies that g is not Carmichael in K by Theorem 3.1. We conclude the proof by noticing that there are infinitely many choices of polynomials G, H . \square

Similar as Theorem 5.1, we have:

Theorem 5.3. *Let g be a rigid Carmichael polynomial of order d in $\mathbb{F}_q[t]$. Then, g is Carmichael in any finite extension over $\mathbb{F}_q(t)$ with degree d whose discriminant is relatively prime to g .*

We now answer the question about the infinitude of Carmichael elements in any function field.

Corollary 5.4. *For any finite extension K over $\mathbb{F}_q(t)$, there are infinitely many Carmichael elements in K .*

Proof. Fix a positive integer $d \geq 2$. Let K be an arbitrary finite extension over $\mathbb{F}_q(t)$ of degree d . Let m be the least common multiple of $1, \dots, d$. Denote by $S(m)$ the set of polynomials which are the product of m distinct irreducible polynomials of the same degree. As in the proof of Theorem 4.8, each polynomial in $S(m)$ is a rigid Carmichael polynomial of order d in $\mathbb{F}_q[t]$. Obviously, there are infinitely many polynomials in $S(m)$ relatively prime to $\text{Disc}(K)$. We conclude the proof by using Theorem 5.3. \square

From now on, we consider the case of non-Carmichael square-free polynomials in $\mathbb{F}_q[t]$.

The following result suggests that a non-Carmichael square-free polynomial can be Carmichael in infinitely many function fields.

Theorem 5.5. *Let $g \in \mathbb{F}_q[t]$ be a square-free polynomial. Let ℓ be any prime factor of $q - 1$ (it requires $q \geq 3$). Let P_i ($1 \leq i \leq s$) be all the monic irreducible factors of g whose degrees do not divide the degree of g , and we further assume that $\deg P_i = \ell$ ($1 \leq i \leq s$). Then, there exist infinitely many cyclic extensions of degree ℓ whose discriminants are relatively prime to g such that g is Carmichael in them.*

Proof. From Dirichlet's theorem on primes in arithmetic progressions in $\mathbb{F}_q[t]$ (see [15, Theorem 4.8]), there exist infinitely many irreducible monic polynomials Q of even degree such that Q is relatively prime to g and

$$\left(\frac{P_i}{Q}\right)_\ell = 1 \quad (1 \leq i \leq s),$$

where $(\cdot)_\ell$ be the ℓ -th power residue symbol in $\mathbb{F}_q[t]$ (see [15, page 24]). From the ℓ -th power reciprocity law in $\mathbb{F}_q[t]$ (see [15, Theorem 3.3]), we have $\left(\frac{Q}{P_i}\right)_\ell = 1$ ($1 \leq i \leq s$) by noticing $\deg Q$ is even. Using [15, Proposition 10.5], each P_i ($1 \leq i \leq s$) splits completely in

$K = \mathbb{F}_q(t)(\sqrt[\ell]{Q})$. Thus, if \mathfrak{p} is any prime factor of $g\mathcal{O}_K$ lying above some P_i ($1 \leq i \leq s$), we have $f(P_i) = 1$ and

$$N_K(\mathfrak{p}) - 1 = q^{\deg P_i} - 1 = q^\ell - 1 \mid q^{\ell \deg g} - 1 = N_K(g\mathcal{O}_K) - 1.$$

If \mathfrak{p} is any prime factor of $g\mathcal{O}_K$ lying above a monic irreducible factor P of g such that $P \neq P_i$ ($1 \leq i \leq s$). Then, we have $\deg P \mid \deg g$ by assumption, and so

$$N_K(\mathfrak{p}) - 1 = q^{f(P)\deg P} - 1 \mid q^{\ell \deg g} - 1 = N_K(g\mathcal{O}_K) - 1,$$

where $f(P)$ is the residue class degree of P in $K/\mathbb{F}_q(t)$ and $f(P) \mid \ell$. Hence, by Theorem 3.1, g is Carmichael in K . \square

As one can imagine, a non-Carmichael square-free polynomial in $\mathbb{F}_q[t]$ is more likely not to be Carmichael in infinitely many function fields. We confirm this by constructing two kinds of function fields: Kummer function fields and cyclotomic function fields.

Theorem 5.6. *Let $g \in \mathbb{F}_q[t]$ be a non-Carmichael square-free polynomial. Let ℓ be any prime factor of $q - 1$. Then, there exists infinitely many cyclic extensions of degree ℓ whose discriminants are relatively prime to g such that g is not Carmichael in them.*

Proof. Since $g \in \mathbb{F}_q[t]$ is a non-Carmichael square-free polynomial, by Theorem 4.1 g has a monic irreducible factor, say P , such that $\deg P \nmid \deg g$.

Let η be a primitive ℓ -th root of unity in \mathbb{F}_q^* . As before, there exist infinitely many irreducible monic polynomials Q of even degree such that Q is relatively prime to g and $\left(\frac{P}{Q}\right)_\ell = \eta$. From the ℓ -th power reciprocity law of $\mathbb{F}_q[t]$ and noticing $\deg Q$ is even, we have $\left(\frac{Q}{P}\right)_\ell = \eta$. Using [15, Proposition 10.5] and noticing $\eta \neq 1$, we know that P is inert in $K = \mathbb{F}_q(t)(\sqrt[\ell]{Q})$. For the prime ideal \mathfrak{p} in K lying above P , noticing $\deg P \nmid \deg g$ we have

$$N_K(\mathfrak{p}) - 1 = q^{\ell \deg P} - 1 \nmid q^{\ell \deg g} - 1 = N_K(g\mathcal{O}_K) - 1.$$

Hence, from Theorem 3.1, g is not Carmichael in K . \square

Note that Theorem 5.6 does not cover the case when $q = 2$. We supplement this by using cyclotomic function fields. First we recall briefly the definition of cyclotomic function fields.

Let $\overline{\mathbb{F}_q(t)}$ be the algebraic closure of $\mathbb{F}_q(t)$. Let $\text{End}(\overline{\mathbb{F}_q(t)})$ be the ring of \mathbb{F}_q -algebra endomorphism of $\overline{\mathbb{F}_q(t)}$. Let

$$\rho : \mathbb{F}_q[t] \rightarrow \text{End}(\overline{\mathbb{F}_q(t)}), \quad M \mapsto \rho_M$$

be the ring homomorphism defined by

$$\rho_a(\alpha) = a\alpha, \quad \rho_t(\alpha) = t\alpha + \alpha^q,$$

where $a \in \mathbb{F}_q$ and $\alpha \in \overline{\mathbb{F}_q(t)}$. For any non-constant polynomial $M \in \mathbb{F}_q[t]$, define

$$\Lambda_M = \{\alpha \in \overline{\mathbb{F}_q(t)} : \rho_M(\alpha) = 0\}.$$

Then, the function field generated by Λ_M over $\mathbb{F}_q(t)$ is called the M -th cyclotomic function field, denoted by $\mathbb{F}_q(t)(\Lambda_M)$. Note that the degree of $\mathbb{F}_q(t)(\Lambda_M)$ over $\mathbb{F}_q(t)$ is equal to $\Phi(M) = |(\mathbb{F}_q[t]/M\mathbb{F}_q[t])^*|$, where Φ is the Euler ϕ -function in $\mathbb{F}_q[t]$ (see [15, page 5]). In [15, Chapter 12] and [20, Chapter 12] there are nice expositions to the arithmetic of cyclotomic function fields.

We also need a result of Bilharz [4] on Artin's primitive root conjecture in function fields; see [15, Chapter 10] for more details.

Theorem 5.7 (Bilharz). *Let K be a function field and α an element of K^* . Then, there are infinitely many prime ideals \mathfrak{p} in K for which α is a primitive root provided that there is no prime factor ℓ of $q - 1$ such that α is an ℓ -th power.*

We are now ready to present our final result.

Theorem 5.8. *Let $g \in \mathbb{F}_q[t]$ be a non-Carmichael square-free polynomial. Then, there exist infinitely many cyclotomic function fields whose discriminants are relatively prime to g such that g is not Carmichael in them.*

Proof. By assumption, g has an irreducible monic factor, say P , such that $\deg P \nmid \deg g$. By Theorem 5.7, there exist infinitely many irreducible monic polynomials Q relatively prime to g such that P is a

primitive root modulo Q . Fix any such Q , and let $K = \mathbb{F}_q(t)(\Lambda_Q)$. By [15, Theorem 12.10], the residue class degree $f(P)$ of P in $K/\mathbb{F}_q(t)$ is the smallest integer such that $P^{f(P)} \equiv 1 \pmod{Q}$. Note that P is a primitive root modulo Q . So, $f(P) = \Phi(Q) = [K : \mathbb{F}_q(t)]$, and thus P is inert in $K/\mathbb{F}_q(t)$. For the unique prime ideal \mathfrak{p} in K lying above P , noticing $\deg P \nmid \deg g$ we obtain

$$N_K(\mathfrak{p}) - 1 = q^{\Phi(Q) \deg P} - 1 \nmid q^{\Phi(Q) \deg g} - 1 = N_K(g\mathcal{O}_K) - 1.$$

Hence, by Theorem 3.1, g is not Carmichael in K . \square

ACKNOWLEDGEMENT

This work was supported by the National Natural Science Foundation of China, Grant No. 11501212. The research of Min Sha was also supported by the Macquarie University Research Fellowship.

REFERENCES

- [1] W.R. Alford, A. Granville and C. Pomerance, There are infinitely many Carmichael numbers, *Ann. Math.* 139 (1994), 703–722.
- [2] T.M. Apostol, *Introduction to analytic number theory*, Springer, New York, 1976.
- [3] W.D. Banks and C. Pomerance, On Carmichael numbers in arithmetic progressions, *J. Aust. Math. Soc.* 88 (2010), 313–321.
- [4] H. Billharz, Primdivisoren mit vorgegebener Primitivwurzel, *Math. Ann.* 114 (1937), 476–492.
- [5] P. Erdős, On pseudoprimes and Carmichael numbers, *Publ. Math. Debrecen.* 4 (1956), 201–206.
- [6] G. Harman, On the number of Carmichael numbers up to x , *Bull. Lond. Math. Soc.* 37 (2005), 641–650.
- [7] G. Harman, Watt’s mean value theorem and Carmichael numbers, *Int. J. Number Theory* 4 (2008), 241–248.
- [8] E.W. Howe, Higher-order Carmichael numbers, *Math. Comp.* 69 (2000), 1711–1719.
- [9] C. Hsu, On Carmichael polynomials, *J. Number Theory* 71 (1998), 257–274.
- [10] N. Jacobson, Structure theory for algebraic algebras of bounded degree, *Ann. Math.* 46 (1945), 695–707.
- [11] W. Knödel, Eine obere Schranke für die Anzahl der Carmichaelschen Zahlen kleiner als x , *Arch. Math.* 4 (1953), 282–284.
- [12] K. Matomäki, On Carmichael numbers in arithmetic progressions, *J. Aust. Math. Soc.* 94 (2013), 268–275.
- [13] P. Pollack, Irreducible polynomials with several prescribed coefficients, *Finite Fields Appl.* 22 (2013), 70–78.
- [14] G. Robin, Grandes valeurs de la fonction somme des diviseurs et hypothèse de Riemann, *J. Math. Pures Appl.* 63 (1984), 187–213.

- [15] M. Rosen, Number theory in function fields, Springer-Verlag, New York, 2002.
- [16] R. Scheidler, Ideal arithmetic and infrastructure in purely cubic function fields, J. Théor. Nombres Bordeaux 13 (2001), 609–631.
- [17] J. Schettler, Lehmer’s totient problem and Carmichael numbers in a PID, available at <http://web.math.ucsb.edu/~jcs/Schettler.pdf>.
- [18] N.J.A. Sloane, The On-Line Encyclopedia of Integer Sequences, <https://oeis.org/A002997>.
- [19] G.A. Steele, Carmichael numbers in number rings, J. Number Theory 128 (2008), 910–917.
- [20] G.D. Villa Salvador, Topics in the theory of algebraic function fields, Birkhäuser, Boston, 2006.
- [21] T. Wright, Infinitely many Carmichael numbers in arithmetic progressions, Bull. London Math. Soc. 45 (2013), 943–952.
- [22] T. Wright, Factors of Carmichael numbers and a weak k -tuples conjecture, J. Aust. Math. Soc. 100 (2016), 421–429.

DEPARTMENT OF MATHEMATICAL SCIENCES, KOREA ADVANCED INSTITUTE OF SCIENCE AND TECHNOLOGY (KAIST), DAEJEON 305-701, REPUBLIC OF KOREA

E-mail address: shbae@kaist.ac.kr

DEPARTMENT OF MATHEMATICS, SOUTH CHINA UNIVERSITY OF TECHNOLOGY, GUANGZHOU 510640, CHINA

E-mail address: mahusu@scut.edu.cn

DEPARTMENT OF COMPUTING, MACQUARIE UNIVERSITY, SYDNEY, NSW 2109, AUSTRALIA

E-mail address: shamin2010@gmail.com