Zhengjun Zhao; Xia Wu

On the subfields of cyclotomic function fields

Czechoslovak Mathematical Journal, Vol. 63 (2013), No. 3, 799–803

Persistent URL: `http://dml.cz/dmlcz/143490`

Czechoslovak Mathematical Journal, 63 (138) (2013), 799–803

ON THE SUBFIELDS OF CYCLOTOMIC FUNCTION FIELDS

Zhengjun Zhao, Anqing, Xia Wu, Nanjing

(Received June 1, 2012)

Abstract. Let $K=\mathbb{F}_q(T)$ be the rational function field over a finite field of q elements. For any polynomial $f(T)\in\mathbb{F}_q[T]$ with positive degree, denote by Λ_f the torsion points of the Carlitz module for the polynomial ring $\mathbb{F}_q[T]$. In this short paper, we will determine an explicit formula for the analytic class number for the unique subfield M of the cyclotomic function field $K(\Lambda_P)$ of degree k over $\mathbb{F}_q(T)$, where $P\in\mathbb{F}_q[T]$ is an irreducible polynomial of positive degree and $k>1$ is a positive divisor of $q-1$. A formula for the analytic class number for the maximal real subfield M^+ of M is also presented. Futhermore, a relative class number formula for ideal class group of M will be given in terms of Artin L-function in this paper.

Keywords: cyclotomic function fields; L-function; class number formula

MSC 2010: 11R18, 11R58, 11R60

1. Introduction

Let $K=\mathbb{F}_q(T)$ be the rational function field over a finite field $\mathbb{F}_q$ of q elements where $q=p^n$ and prime p is the characteristic of $\mathbb{F}_q$. Throughout this paper, assume that p is an odd prime. Let P be a monic irreducible polynomial of degree $d>0$ in $\mathcal{O}_K=\mathbb{F}_q[T]$, $K_P=K(\Lambda_P)=K(\lambda_P)$ a cyclotomic function field where Λ_P is the set of P-torsion elements in the Carlitz $\mathcal{O}_K$-module $\overline{K}$ (here $\overline{K}$ is the algebraic closure of K) and λ_P a fixed choice of primitive P-torsion element in Λ_P, and $K_P^+=K(\Lambda_P)^+$ the maximal real subfield of K_P. It is well known that K_P/K and K_P^+/K are cyclic extensions of function fields. Let $C_a(x)$ be the Carlitz polynomial for $0\neq a\in\mathcal{O}_K$. The Galois group $\mathrm{Gal}(K_P/K)$ is canonically isomorphic to the multiplicative group $(\mathcal{O}_K/(P))^*$ by $\sigma_a\mapsto a \pmod P$ for $a\in\mathcal{O}_K$, $(a,P)=1$, where σ_a is the automorphism determined by $\sigma_a\lambda_P=C_a(\lambda_P)$. Denote the set

This work was supported by NSFC (No. 11301071), CPSF (No. 2013M531244) and NSFJ (No. 1202101c).

$\{\sigma_\alpha \in \mathrm{Gal}(K_P/K)\colon\ \alpha \in \mathbb{F}_q^*\}$ by J. Then the field K_P^+ is the fixed field of the group J in K_P, and $\mathrm{Gal}(K_P^+/K) \cong (\mathcal{O}_K/(P))^*/\mathbb{F}_q^*$.

Having introduced the above notations and definitions, we now briefly describe our main results. Since the Galois group $\mathrm{Gal}(K_P/K)$ is a cyclic group of order q^d-1, there is a unique subfield $M \subset K_P$ such that $[M:K]=k$ for any positive integer $k \mid q^d-1$. Furthermore, if k divides $q-1$, we can get an explicit form of M, which is the content of Proposition 2.1. For the rest of this paper, let k be a fixed positive integer with $k \mid q-1$ and M the subfield of K_P of degree k over K. Let $M^+ = M \cap K_P^+$, we will call it the maximal real subfield of M. The explicit formulas for the analytic class number for M and M^+ will be presented in the Theorem 2.5 in the following section.

2. Main results

There are many papers concerned with the class numbers of cyclotomic function fields (see e.g. [1], [2], [3], [4], [6], et al.). With the notations defined in the previous section, we will consider the formulas for the analytic class number for M and M^+. To ease notation, we denote by $\mathcal{M}$ the set of monic polynomials of degree less than d in $\mathcal{O}_K$. The following proposition gives the specific form of M.

Proposition 2.1. *If the degree d of P is even, then $M = K(\sqrt[k]{P})$; otherwise $M = K(\sqrt[k]{-P})$.*

Proof. For the Carlitz polynomial $C_P(x)$, we know from Proposition 3.2.6 in [7] that $C_P(x)/x$ is the minimal polynomial of P over K, and $C_P(x)/x = \prod\limits_{0\neq\lambda\in\Lambda_P}(x-\lambda)$.

It is easy to see that the set of non-zero elements of Λ_P coincides with $\{\sigma_a\lambda_P\colon\ 0 \neq a \in \mathcal{O}_K,\ \deg a < d\}$. Since every non-zero polynomial in $\mathcal{O}_K$ can be written uniquely as the product of a constant times a monic one, we can get the following equation

$$\Bigl(\prod_{\alpha\in\mathbb{F}_q^*}\alpha\Bigr)^{(q^d-1)/(q-1)} \prod_{a\in\mathcal{M}}(\sigma_a\lambda_P)^{q-1} = P.$$

Note here that $\prod\limits_{\alpha\in\mathbb{F}_q^*}\alpha = -1$ by the theory of finite fields, and $x^k \pm P$ are irreducible polynomials over K. When d is an even number, we claim that $(q^d-1)/(q-1)$ is even, and thus $\Bigl(\prod\limits_{\alpha\in\mathbb{F}_q^*}\alpha\Bigr)^{(q^d-1)/(q-1)} = 1$. In this case, we obtain that $K(\sqrt[k]{P})$ is the unique subfield of K_P of degree k over K. If d is odd, we get $\prod\limits_{a\in\mathcal{M}}(\sigma_a\lambda_P)^{q-1} = -P$, and thus $K(\sqrt[k]{-P})$ is the unique subfield of K_P of degree k over K. This completes our proof. $\square$

Actually, we can say more about the above subfield M of K_P. To prove our next theorem, we give an easy result from elementary number theory.

Lemma 2.2. *Let q, d and k be positive integers with $q > 1$ and k dividing both $q-1$ and d. Then $(q^d-1)/(q-1) \equiv 0 \pmod{k}$.*

Proof. Set $d = d_1 k$. Note that $\frac{q^d-1}{q-1} = \frac{q^{d_1}-1}{q-1}(q^{d_1(k-1)} + \ldots + q^{d_1} + 1)$. Combining this equality with the condition $k \mid q-1$ yields our conclusion. $\square$

Theorem 2.3. *$M \subseteq K_P^+$ if and only if $k \mid d$.*

Proof. First, we address the case when d is even, i.e., $M = K(\sqrt[k]{P})$ by Proposition 2.1. Suppose that $M \subseteq K_P^+$. We note that the infinite prime $\infty = 1/T$ of K splits completely in M/K. For any prime $\mathfrak{p}_\infty$ of M lying over ∞, $\operatorname{ord}_{\mathfrak{p}_\infty}(\sqrt[k]{P}) = \operatorname{ord}_\infty(P)/k = -d/k$, and thus $k \mid d$.

Conversely, we assume that $k \mid d$. By the proof of Proposition 2.1, we assert that $\Big(\prod\limits_{a\in\mathcal{M}} \sigma_a\lambda_P\Big)^{q-1} = P$. Thus, there is some $\beta \in (\mathbb{F}_q^*)^{(q-1)/k}$ such that $\sqrt[k]{P} = \beta\Big(\prod\limits_{a\in\mathcal{M}} \sigma_a\lambda_P\Big)^{(q-1)/k}$. For any element $\alpha \in \mathbb{F}_q^*$,

$$\begin{aligned}\sigma_\alpha(\sqrt[k]{P}) &= \sigma_\alpha\bigg(\beta\Big(\prod_{a\in\mathcal{M}} \sigma_a\lambda_P\Big)^{(q-1)/k}\bigg) = \beta\Big(\prod_{a\in\mathcal{M}} \alpha\sigma_a\lambda_P\Big)^{(q-1)/k} \\ &= \beta(\alpha^{(q^d-1)/(q-1)})^{(q-1)/k}\Big(\prod_{a\in\mathcal{M}} \sigma_a\lambda_P\Big)^{(q-1)/k} \qquad \text{(using 2.2)} \\ &= \sqrt[k]{P}.\end{aligned}$$

Then, by definition of K_P^+, we can claim that $M \subseteq K_P^+$.

The proof for the case when d is odd, i.e., $M = K(\sqrt[k]{-P})$, is done analogously and we omit it here for concision. $\square$

Denote by r the greatest common divisor of d and k. It is not hard to show that r is exactly the degree of M^+ over K.

Corollary 2.4. $[M^+ : K] = r$.

Proof. Let N be the unique subfield of K_P of degree r over K. Combining the fact that $r \mid d$ and $r \mid k$ with Theorem 2.3, we can assert that N is contained in both M and K_P^+, and thus $N \subseteq M^+$. Therefore, $r \leqslant [M^+ : K]$. The fact that $M^+ = M \cap K_P^+$ yields that $[M^+ : K] \mid r$, and this completes our proof. $\square$

Before presenting formulas for the analytic class number for M and M^+, we have to introduce some notations and terminologies. Denote by S_M and S_{M^+} respectively the sets of primes of M and M^+ lying above ∞. Let $\mathcal{O}_M$ and $\mathcal{O}_{M^+}$ denote the rings of integers of M and M^+ associated to S_M and S_{M^+}, respectively. Note that the cardinalities of S_M and S_{M^+} are equal to r. Denote by $h(\mathcal{O}_M)$ and $h(\mathcal{O}_{M^+})$ the ideal class number of $\mathcal{O}_M$ and $\mathcal{O}_{M^+}$, respectively. Denote by h_M and h_{M^+} the order of the group of divisor classes of degree zero of M and M^+, respectively.

Based on the relation of zeta functions and Artin L-functions of M and M^+, we can get the following theorem which is the main result of this paper.

Theorem 2.5. *Let M denote the subfield of K_P of degree k over K and M^+ the maximal real subfield of M, we have*

$$h_{M^+} = \prod_{\substack{\chi\neq\chi_0 \\ \chi \text{ even}}} \Big(\sum_{a\in\mathcal{M}} -\chi(a)\deg(a) \Big),$$

and

$$h_M = \prod_{\chi \text{ odd}} \Big(\sum_{a\in\mathcal{M}} \chi(a) \Big) \prod_{\substack{\chi\neq\chi_0 \\ \chi \text{ even}}} \Big(\sum_{a\in\mathcal{M}} -\chi(a)\deg(a) \Big),$$

where the χ in the above formulas is non-trivial character of $\mathrm{Gal}(M/K)$.

Proof. Note that all characters of $\mathrm{Gal}(K_P/K)$ corresponding to M/K are even and the cardinalities of S_M and S_{M^+} are equal to r, the result follows as in the proof of Theorem 16.8 in [5]. □

Two facts h_M/h_{M^+} is a rational number and $\prod_{\chi \text{ odd}} \Big(\sum_{a\in\mathcal{M}} \chi(a) \Big)$ is an algebraic integer yield that h_M/h_{M^+} is a rational integer, and thus $h_{M^+} \mid h_M$.

It is easy to see that the extension M/M^+ is totally imaginary extension of function fields. In other words, every prime in S_{M^+} has only one prime above it in M. In fact, all primes in S_{M^+} are totally ramified in M/M^+. By the Theorem 3.1 of [6], we know that $\mathcal{O}_M^* = \mathcal{O}_{M^+}^*$ and $h(\mathcal{O}_{M^+})$ divides $h(\mathcal{O}_M)$. Set $h^-(\mathcal{O}_M) = h(\mathcal{O}_M)/h(\mathcal{O}_{M^+})$, we have

Theorem 2.6. *With notations defined as above,*

$$h^-(\mathcal{O}_M) = \Big(\frac{r}{k}\Big)^{r-1} \prod_{\chi \text{ odd}} L_{S_{M^+}}(0,\chi),$$

where χ in the product runs over all odd characters of $\mathrm{Gal}(M/K)$, *and $L_{S_{M^+}}(\omega,\chi)$ is S_{M^+}-L-function for M/M^+.*

P r o o f. This follows from Theorem 4.5 in [6]. □

Acknowledgement. The authors would like to express their sincere gratitude to their adviser Professor Qin Hourong for many helpful suggestions. The authors also want to express their thanks to the referees for their careful reading of the manuscript and suggestions on the writing of the paper.

References

[1] *S. Bae, P.-L. Lyun*: Class numbers of cyclotomic function fields. Acta. Arith. *102* (2002), 251–259.
[2] *S. Galovich, M. Rosen*: Units and class groups in cyclotomic function fields. J. Number Theory *14* (1982), 156–184.
[3] *L. Guo, S. Linghsuen*: Class numbers of cyclotomic function fields. Trans. Am. Math. Soc. *351* (1999), 4445–4467.
[4] *D. R. Hayes*: Analytic class number formulas in global function fields. Invent. Math. *65* (1981), 49–69.
[5] *M. Rosen*: Number Theory in Function Fields. Graduate Texts in Mathematics 210. Springer, New York, 2002.
[6] *M. Rosen*: The Hilbert class field in function fields. Expo. Math. *5* (1987), 365–378.
[7] *Z. Z. Zhao*: The Arithmetic Problems of Some Special Algebraic Function Fields. Ph.D. Thesis, NJU, 2012. (In Chinese.)

Authors' addresses: Zhengjun Zhao (corresponding author), School of Mathematics and Computational Science, Anqing Normal University, Anqing 246133, People's Republic of China, e-mail: zywnju@gmail.com; Xia Wu, Department of Mathematics, Southeast University, Nanjing 210096, People's Republic of China, e-mail: xiaxia80@gmail.com.