Vol. 35 (2015)
No. 5

数 学 杂 志
J. of Math. (PRC)

AMBIGUOUS CLASSES OF SOME CYCLIC ALGEBRAIC FUNCTION FIELDS

ZHANG Feng

(*Department of Mathematics, Hebei North University, Zhangjiakou 075000, China*)

Abstract: We study the structure of some kinds of cyclic function fields with degree l. By the means of prime ideal decomposition and the computation of first cohomology of the ideal class group, we get the lower bound of the l-ranks of the class group of these function fields. In addition, we find a necessary condition on when these kinds of fields have ambiguous class containing no ambiguous ideals.

Keywords: cyclic function fields; ambiguous class; class group

2010 MR Subject Classification: 11R18; 11R29

Document code: A **Article ID:** 0255-7797(2015)05-1035-07

1 Introduction

Let $k = \mathbb{F}_q(T)$ be the rational function field with constant field $\mathbb{F}_q$, the finite field with q elements, where q is a power of an odd prime number. The set $R = \mathbb{F}_q[T]$ of all the polynomials of T over $\mathbb{F}_q$ is called the integral domain of k. A finite extension of k is called an algebraic function field. Let $l \leq 19$ be a prime number such that $l|(q-1)$. The function fields $k(\sqrt[l]{(D(T)})$ (where $D(T)$ are not the l-th power of any polynomial) are l-th cyclic function fields. Artin studied the case $l = 2$ systematically in [1]. By the discussing of ambiguous ideal classes Zhang (see [2]) explicitly expressed the 2-rank of the class group of $k(\sqrt{(D(T)})$ and gave a necessary and sufficient condition for the class number to be odd. Zhang's result was used by Ma and Feng (see [3]) to study the ideal class groups of imaginary quadratic function fields. They obtained a condition for the ideal class groups having exponent ≤ 2.

Here we study the general l-th function fields $K = k(\sqrt[l]{D})$, where $2 < l \leq 19$. Denote the Galois group of K/k as $\mathrm{Gal}(K/k) = \langle\sigma\rangle = \{1, \sigma, \sigma^2, \cdots, \sigma^{l-1}\}$. The integral closure of R in K (denoted as $\mathcal{O}_K$) is called the integral domain of K. The invertible elements (units) of $\mathcal{O}_K$ constitute a group U_K, the unit group of K or $\mathcal{O}_K$.

K is called a real l-th function field if D is monic and the degree of the polynomial D is a multiple of l, otherwise, we call K a imaginary function field. In the real case, $U_K = \mathbb{F}_q^\times \times V_K$, where V_K is a free abelian group with rank $l-1$. A set of generators of it is called a basic

* **Received date:** 2013-01-11 **Accepted date:** 2013-04-01

Foundation item: Supported by National Natural Science Foundation of China (60970153).

Biography: Zhang Feng (1971–), male, born at Zhangjiakou, Hebei, lecturer, major in number theory.

system of units. Let $U_K = \mathbb{F}_q^\times \times V_K$, where V_K is a free abelian group with rank $l-1$. If there is an element ε of U_K satisfying

$$V_K = \langle \varepsilon, \varepsilon^\sigma, \varepsilon^{\sigma^2}, \cdots, \varepsilon^{\sigma^{l-2}} \rangle,$$

then ε is called a Minkowski unit of K. It is known (see [4]) that has Minkowski unit if l is a prime number ≤ 19. Here and afterward, we assume that l is a prime number ≤ 19.

Similar to number fields, the set $\mathcal{I}(K)$ of fractional ideals of K is a group with respect to the multiplication of ideals. All the principal fractional ideals constitute a subgroup $\mathcal{P}(K)$ of $\mathcal{I}(K)$, the so called principal ideal subgroup. The quotient group $H(\mathcal{O}_\mathcal{K}) = \mathcal{P}(\mathcal{K})/\mathcal{I}(\mathcal{K})$ is called the ideal class group of K. An ideal class containing ideal $\mathfrak{a}$ is denoted as $[\mathfrak{a}]$. It is a classical result that the ideal class group of K is a finite abelian group. From the study of the properties and the constructions of the ambiguous ideal classes we'll prove the following theorems.

Theorem 1.1 Let $K = k(\sqrt[l]{D})$ with $D = aP_1(T)^{\alpha_1} P_2(T)^{\alpha_2} \cdots P_s(T)^{\alpha_s}$, where $a \in \mathbb{F}_q^\times$, $P_1(T), P_2(T), \cdots, P_s(T)$ are irreducible polynomials in $\mathbb{F}_q[T]$ and $1 \le \alpha_1, \alpha_2, \cdots, \alpha_s < l$. Then we have

$$\mathrm{Rank}_l H(\mathcal{O}_K) \ge \begin{cases} s-2, & \text{if } K \text{ is real and } \ \mathrm{N}\varepsilon = 1; \\ s-1, & \text{otherwise.} \end{cases}$$

Theorem 1.2 Suppose that $K = k(\sqrt[l]{D})$ is a real l-th cyclic function field and $\mathrm{N}\varepsilon = 1$. If $D = X^l - gY^l$ (where $X, Y \in R$, g is a generator of $\mathbb{F}_q^\times$), then the ideal class group of K has an ambiguous class not containing any ambiguous ideal.

2 The Proofs of Lemmas and Theorems

Definition 2.1 An ideal $\mathfrak{a}$ of K is called an ambiguous ideal of K if $\mathfrak{a}^\sigma = \mathfrak{a}$. An ideal class $[\mathfrak{a}]$ of K is called ambiguous if $[\mathfrak{a}]^\sigma = [\mathfrak{a}]$.

An ambiguous class is of order 1 or l: if an ambiguous ideal class $[\mathfrak{a}] \ne [1]$, then

$$\begin{aligned} [\mathfrak{a}]^l &= [\mathfrak{a}] \cdot [\mathfrak{a}]^\sigma \cdots [\mathfrak{a}]^\sigma \\ &= [\mathfrak{a}] \cdot [\mathfrak{a}]^\sigma \cdots [\mathfrak{a}]^{\sigma^2} \\ &= \cdots\cdots \\ &= [\mathfrak{a}] \cdot [\mathfrak{a}]^\sigma \cdots [\mathfrak{a}]^{\sigma^{l-1}} \\ &= [\mathrm{N}\mathfrak{a}] \\ &= [1]. \end{aligned}$$

Assume that $D = P_1^{\alpha_1} P_2^{\alpha_2} \cdots P_s^{\alpha_s}$, then the principal ideal (P_i) of k factors as $(P_i) = \mathfrak{P}_i^l$ $(i = 1, 2, \cdots, s)$ in K. It is obvious that the ideals

$$\prod_{i=1}^{s} \mathfrak{P}_i^{s_i} \ (s_i \in \{0, 1, \cdots, l-1\}) \quad \text{and} \quad (1), \quad (\sqrt[l]{D_i}) \ (i \in \{1, \cdots, l-1\})$$

are all ambiguous ideals of K, here D_i is the l-free part of D^i. In addition, if K is a real l-th cyclic function field and its Minkowski unit ε satisfies $\mathrm{N}_{K/k}\varepsilon = 1$, from Hilbert theorem 90, there is an element $\gamma \in \mathcal{O}_K$ such that $\varepsilon = \gamma/\gamma^\sigma$. Under this condition,

$$(\gamma^i) \text{ and } (\gamma^i \sqrt[l]{D_j}) \ (i, j \in \{0, 1, \cdots, l-1\})$$

are also ambiguous ideals of K.

In fact, we have listed all the ambiguous ideals of K:

Lemma 2.2 If an ambiguous ideal $\mathcal{A}$ of K does not have rational factors, it must be of the form

$$\mathcal{A} = \prod_{i=1}^{s} \mathfrak{P}_i^{s_i}, \quad \text{where } \mathfrak{P}_i | P_i, \ s_i \in \{0, 1, \cdots, l-1\}.$$

Proof Let $\mathcal{A}$ be an unprincipal ambiguous ideal without rational factors. It factors as

$$\mathcal{A} = \prod_{i \in I} \mathfrak{P}_i^{a_i} \prod_{j \in J} \mathfrak{Q}_j^{b_j},$$

where $\mathfrak{P}_i$'s are ramified prime ideals and $\mathfrak{Q}_j$'s are splitting ones. From the definition of 'ambiguous', we know that

$$\mathcal{A} = \mathcal{A}^\sigma = \prod_{i \in I} \mathfrak{P}_i^{a_i} \prod_{j \in J} \bar{\mathfrak{Q}}_j^{b_j},$$

where $\bar{\mathfrak{Q}} = \mathfrak{Q}^\sigma$. The uniqueness of factorization leads to $b_j = 0, \forall j \in J$.

Lemma 2.3 A principal ambiguous ideal without rational factors must be of the following forms:

(1) $(\sqrt[l]{D_i})$ $(i \in \{0, 1, \cdots, l-1\})$;

(2) if K is a real l-th cyclic function field and its Minkowfski unit ε satisfies $\mathrm{N}_{K/k}\varepsilon = 1$, then ε can be written as $\varepsilon = \gamma/\gamma^\sigma$. Whence (γ^i) and $(\gamma^i \sqrt[l]{D_j})$ $(i \in \{0, 1, \cdots, l-1\}, j \in \{1, \cdots, l-1\})$ are principal ambiguous ideals of K.

Proof If (z) is a principal ambiguous ideal without rational factors, where $z \in \mathcal{O}_K$, then $(z) = (z)^\sigma$. This means that $z/z^\sigma = u \in U_K$, and $\mathrm{N}u = 1$.

Case 1 Suppose that K is imaginary. Then $u \in \mathbb{F}_q^\times = \langle g \rangle$ and there exists a positive integer m such that $u = g^{\frac{q-1}{l}m}$ $(m \in \{1, \cdots, l-1\})$. Without lost of generality, we can choose that $\sqrt[l]{D}^\sigma = g^{\frac{1-q}{l}} \sqrt[l]{D}$. So we have

$$\sqrt[l]{D_m}^\sigma = g^{\frac{1-q}{l}m} \sqrt[l]{D_m} = u^{-1} \sqrt[l]{D_m}.$$

It follows that

$$z/\sqrt[l]{D_m} = z^\sigma u/\sqrt[l]{D_m} = \left(z/\sqrt[l]{D_m}\right)^\sigma,$$

and so $z/\sqrt[l]{D_m} \in k$. Because (z) does not have rational factors, we have $(z) = (\sqrt[l]{D_m})$.

Case 2 Assume that K is a real function field and $\mathrm{N}(\varepsilon) = g^m \neq 1$ (where ε is the Minkowski unit of K). Suppose, without lost of generality, let $m \in \{1, 2, \cdots, l-1\}$. Then

$$u = c\varepsilon_0^{a_0} \varepsilon_1^{a_1} \cdots \varepsilon_{l-2}^{a_{l-2}}, \text{ where } c \in \mathbb{F}_q^\times; \quad \varepsilon_i = \varepsilon^{\sigma^i}, a_i \in \mathbb{Z} \ (i = 0, 1, \cdots, l-2).$$

Take norms of both side, we get $1 = \mathrm{N}u = c^l g^{(a_0+a_1+\cdots+a_{l-2})m}$. Hence $l|(a_0+a_1+\cdots+a_{l-2})$.

Set

$$\begin{array}{lllllll} b_{l-2} & = & m(a_0+a_1+\cdots+a_{l-2})/l, & & & \\ \beta_0 & = & b_{l-2}, & b_0 & = & a_0-\beta_0; \\ \beta_1 & = & b_{l-2}-b_0, & b_1 & = & a_1-\beta_1; \\ \cdots & & & \cdots & & \\ \beta_{l-3} & = & b_{l-2}-b_{l-4}, & b_{l-3} & = & a_{l-3}-\beta_{l-3}; \\ \beta_{l-2} & = & b_{l-2}-b_{l-3}. & & & \end{array}$$

Then we have

$$u = c\varepsilon_0^{b_0}\varepsilon_1^{b_1}\cdots\varepsilon_{l-2}^{b_l-2}\varepsilon_0^{\beta_0}\varepsilon_1^{\beta_1}\cdots\varepsilon_{l-2}^{\beta_l-2}.$$

Let

$$\eta_1 = \varepsilon_0^{b_0}\varepsilon_1^{b_1}\cdots\varepsilon_{l-2}^{b_{l-2}}, \qquad \eta_2 = \varepsilon_0^{\beta_0}\varepsilon_1^{\beta_1}\cdots\varepsilon_{l-2}^{\beta_{l-2}}.$$

We know from $\mathrm{N}\varepsilon = g^m$ that $\varepsilon_{l-1} = g^m\varepsilon_0^{-1}\varepsilon_1^{-1}\cdots\varepsilon_{l-2}^{-1}$. It implies that

$$\begin{aligned} \eta_1^\sigma &= \varepsilon_1^{b_0}\varepsilon_2^{b_1}\cdots\varepsilon_{l-1}^{b_{l-2}} \\ &= \varepsilon_1^{b_0}\varepsilon_2^{b_1}\cdots\varepsilon_{l-2}^{b_{l-3}}\cdot g^{mb_{l-2}}\varepsilon_0^{-b_{l-2}}\varepsilon_1^{-b_{l-2}}\cdots\varepsilon_{l-2}^{-b_{l-2}} \\ &= g^{mb_{l-2}}\varepsilon_0^{-b_{l-2}}\varepsilon_1^{b_0-b_{l-2}}\cdots\varepsilon_{l-2}^{b_{l-3}-b_{l-2}} \\ &= g^{mb_{l-2}}\varepsilon_0^{-\beta_0}\varepsilon_1^{-\beta_1}\cdots\varepsilon_{l-2}^{-\beta_{l-2}} \\ &= g^{mb_{l-2}}\eta_2^{-1}. \end{aligned}$$

That is

$$\begin{aligned} &z/z^\sigma = c\eta_1\eta_2 = cg^{mb_{l-2}}\eta_1\eta_1^{-\sigma}, \\ &z/\eta_1 = cg^{mb_{l-2}}(z^\sigma/\eta_1^\sigma) = c'(z/\eta_1)^\sigma, \qquad \text{where} \quad c' \in \mathbb{F}_q^\times. \end{aligned}$$

Similar to Case 1, there is a $s \in \{0, 1, \cdots, l-1\}$ such that

$$(z) = (z/\eta_1) = \left(\sqrt[l]{D}^s\right).$$

Case 3 K is a real function field and $\mathrm{N}(\varepsilon) = 1$. From Hilbert theorem 90, we know that there exists a $\gamma \in \mathcal{O}_K$ such that $\varepsilon = \gamma/\gamma^\sigma$. Denote $\gamma^{\sigma^i} = \gamma_i$, we have

$$\varepsilon_i = \varepsilon^{\sigma_i} = \gamma^{\sigma^i}/\gamma^{\sigma^{i+1}} = \gamma_i/\gamma_{i+1}.$$

Hence

$$z/z^\sigma = u = c\varepsilon_0^{a_0}\varepsilon_1^{a_1}\cdots\varepsilon_{l-2}^{a_{l-2}}, \quad \text{where } c^l = 1.$$

Set $\tilde{\gamma} = \gamma_0^{a_0}\gamma_1^{a_1}\cdots\gamma_{l-2}^{a_{l-2}}$. It follows that

$$z/\tilde{\gamma} = c(z/\tilde{\gamma})^\sigma,$$

and so

$$(z) = (\gamma^s) \quad \text{or} \quad \left(\gamma^s \sqrt[l]{D}^t\right) \text{ where } s, t \in \{1, 2, \cdots, l-1\}.$$

Proof of Theorem 1.1 From the above lemmas the number A of ideal classes containing ambiguous ideals of $K = (\sqrt[l]{aP_1(T)^{\alpha_1} P_2(T)^{\alpha_2} \cdots P_s(T)^{\alpha_s}})$ satisfies

$$A = \begin{cases} l^{s-2} & \text{if } K \text{ is real and } \mathrm{N}\varepsilon = 1; \\ l^{s-1} & \text{otherwise}. \end{cases}$$

This means

$$\mathrm{Rank}_l H(\mathcal{O}_K) \geq \begin{cases} s-2, & \text{if } K \text{ is real and } \mathrm{N}\varepsilon = 1; \\ s-1, & \text{otherwise}. \end{cases}$$

Let's count all the ambiguous ideal classes of K.

Lemma 2.4 Denote the ideal class group of K as $H(\mathcal{O}_K)$. Let $H(\mathcal{O}_K)^G$ express its subgroup consists of all the ambiguous ideal classes. Then

$$\left|H(\mathcal{O}_K)^G\right| = \frac{l^{s+\delta-1}}{(\mathbb{F}_q^\times : \mathrm{N}_{K/k} K^\times \bigcap \mathbb{F}_q^\times)}.$$

where $\delta = \begin{cases} 0, & \text{if } K \text{ is real}; \\ 1, & \text{if } K \text{ is imaginary}. \end{cases}$

Proof For simplicity, we denote the ideal group, the principal ideal group and the ideal class group of field L as I_L, P_L, and C_L respectively. With our field K we have exact sequence (see [5])

$$0 \longrightarrow P_K \longrightarrow I_K \longrightarrow C_K \longrightarrow 0.$$

Because $H^1(\mathrm{G}, I_K) = \oplus_\wp H^1(\mathrm{G}_\wp, \mathbb{Z})$ and $H^1(\mathrm{G}_\wp, \mathbb{Z}) = 1$, we have $H^1(\mathrm{G}, I_K) = 1$. That means that the exact sequence

$$0 \longrightarrow P_K^G \longrightarrow I_K^G \longrightarrow C_K^G \longrightarrow H^1(\mathrm{G}, P_K) \longrightarrow 0$$

holds. It is the same to say that we have the following short exact sequence

$$0 \longrightarrow I_K^G / P_K^G \longrightarrow C_K^G \longrightarrow H^1(\mathrm{G}, P_K) \longrightarrow 0.$$

It follows that

$$\left|C_K^G\right| = (I_K^G : P_K^G) \cdot \# H^1(\mathrm{G}, P_K).$$

But we have $I_K^G \supset P_K^G \supset P_K$, so

$$(I_K^G : P_K^G) = (I_K^G : P_k)/(P_K^G : P_k) = (I_K^G : I_k)/(P_K^G : P_k) = e_0(K)/(P_K^G : P_k),$$

where $e_0(K) = l^s$ is the product of the ramified indices of all the ramified prime ideals of K. It is seen from Hilbert theorem 90 that $H^1(\mathrm{G}, K^\times) = 0$. From the short exact sequence

$$0 \longrightarrow U_K \longrightarrow K^\times \longrightarrow P_K \longrightarrow 0$$

we obtain the long exact sequence

$$0 \longrightarrow U_k \longrightarrow k^\times \longrightarrow P_K^G \longrightarrow H^1(G, U_K) \longrightarrow 0.$$

Moreover, we conclude that

$$0 \longrightarrow P_k \longrightarrow P_K^G \longrightarrow H^1(G, U_K) \longrightarrow 0$$

are exact. It means that

$$(P_K^G : P_k) = \#H^1(G, U_K) = \#H^0(G, U_K)/Q(G, U_K).$$

where the Herband quotient

$$Q(G, U_K) = \frac{1}{l} \prod_{v \in S_\infty} e_v f_v = \frac{1}{l} e_\infty f_\infty = \begin{cases} \frac{1}{l}, & \text{if } K \text{ is real ;} \\ 1, & \text{if } K \text{ is imaginary .} \end{cases}$$

Thus we have

$$(P_K^G : P_k) = \frac{l \cdot \#H^0(G, U_K)}{e_\infty f_\infty} = \begin{cases} l \cdot \#H^0(G, U_K), & \text{if } K \text{ is real ;} \\ \#H^0(G, U_K), & \text{if } K \text{ is imaginary .} \end{cases}$$

On the other hand, we have exact hexagon

$$\begin{array}{ccccc} & H^0(U_K) & \longrightarrow & H^0(K^\times) & \\ \nearrow & & & & \searrow \\ H^1(P_K) & & & & H^0(P_K) \\ \nwarrow & & & & \swarrow \\ & H^1(K^\times) & \longleftarrow & H^1(U_K) & \end{array}$$

and get exact sequence

$$0 = H^1(K^\times) \longrightarrow H^1(P_K) \longrightarrow H^0(U_K) \longrightarrow H^0(K^\times).$$

So

$$\#H^1(P_K) = \#\ker(U_k/\mathrm{N}_{K/k}U_K \longrightarrow k^\times/\mathrm{N}_{K/k}) = (\mathrm{N}_{K/k}(K^\times) \cap U_k : \mathrm{N}_{K/k}(U_K)).$$

But $U_k \supset (\mathrm{N}_{K/k}(K^\times) \bigcap U_k) \supset \mathrm{N}_{K/k}(U_K)$, hence

$$\#H^1(G, P_K) = \#(U_k : \mathrm{N}_{K/k}(U_K))/(U_k : \mathrm{N}_{K/k}(K^\times) \bigcap U_k).$$

It implies that

$$\left|H(\mathcal{O}_K)^G\right| = (I_K^G : P_K^G) \cdot \#H^1(G, P_K) = \frac{e_0 e_\infty f_\infty}{l \cdot (\mathbb{F}_q^\times : \mathrm{N}_{K/k}K^\times \bigcap \mathbb{F}_q^\times)}.$$

Proof of Theorem 1.2 If K is real, then

$$\left|H(\mathcal{O}_K)^G\right| = \frac{l^{s-1}}{(\mathbb{F}_q^\times : \mathrm{N}_{K/k}K^\times \bigcap \mathbb{F}_q^\times)}.$$

If $D = X^l - gY^l$, then

$$\eta = \frac{X}{Y} - \frac{\sqrt{D}}{Y} \in K^* \text{ and } N\eta = g.$$

So $N_{K/k}K^* \bigcap \mathbb{F}_q^\times = \mathbb{F}_q^\times$ and $(H(O_K)^G) = l^{s-1}$.

On the other hand, if $N\varepsilon = 1$, then there are l^{s-2} ambiguous ideals. Thus we can see, in this case, there is an ambiguous ideal class not containing any ambiguous ideal.

References

[1] Artin E. Quadratic Körper im gebiet der Höhren Kongruenzen I, II[J]. Math. Z., 1924, 19: 153–246.

[2] Zhang X. Ambiguous classes and 2-rank of class group of quadratic function fields[J]. Journal of China University of Science and Technology, 1987, 17(4): 425–431.

[3] Ma L, Feng K. On imaginary quadratic function fields with ideal class group of exponent ≤ 2[J]. Chinese Journal of Contemporary Mathematics, 2002, 23(4): 383–388.

[4] Feng K, Cheng L. On the Minkowski unit in function fields[J]. Sci. Bull., 1989, 34: 809–811.

[5] Lang S. Algebraic number theory (sec. edi.) [M]. Berlin: Springer Verlag, 1994.

一些循环代数函数域的不分明理想类

张 峰

(河北北方学院理学院数学系, 河北 张家口 075000)

摘要: 本文研究了一些l次循环函数域的理想类群的不分明理想类的结构问题. 利用函数域的素理想分解理论和理想的一阶上同调理论, 得到了这几类循环函数域的理想类群的l -秩的下界. 进一步, 我们还得了一些不分明理想类中不含不分明理想的域的充分条件.

关键词: 循环函数域; 不分明理想类; 理想类群

MR(2010)**主题分类号**: 11R18; 11R29 **中图分类号**: O156.2