Finite Fields and Their Applications 16 (2010) 255–264

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

The genus fields of Artin–Schreier extensions

Su Hu *, Yan Li

Department of Mathematical Sciences, Tsinghua University, Beijing 100084, China

ARTICLE INFO

Article history:
Received 22 June 2009
Revised 25 March 2010
Available online 9 April 2010
Communicated by H. Stichtenoth

MSC:
primary 11R58
secondary 11R37

Keywords:
Genus field
Artin–Schreier extension
Ambiguous ideal class

ABSTRACT

Let q be a power of a prime number p. Let $k = \mathbb{F}_q(t)$ be the rational function field with constant field $\mathbb{F}_q$. Let $K = k(\alpha)$ be an Artin–Schreier extension of k. In this paper, we explicitly describe the ambiguous ideal classes and the genus field of K. Using these results, we study the p-part of the ideal class group of the integral closure of $\mathbb{F}_q[t]$ in K. We also give an analogue of the Rédei–Reichardt formula for K.

1. Introduction

In 1951, Hasse [7] introduced genus theory for quadratic number fields which is very important for studying the ideal class groups of quadratic number fields. Later, Fröhlich [4] generalized this theory to arbitrary number fields. In 1996, S. Bae and J.K. Koo [3] defined the genus field for global function fields and developed the analogue of the classical genus theory. In 2000, Guohua Peng [8] explicitly described the genus theory for Kummer function fields.

The genus theory for function fields is also very important for studying the ideal class groups of function fields. Let l be a prime number and K be a cyclic extension of degree l of the rational function field $\mathbb{F}_q(t)$ over a finite field of characteristic $\neq l$. In 2004, Wittmann [13] generalized Guohua Peng's results to the case $l \nmid q-1$ and used it to study the l-part of the ideal class group of the integral closure of $\mathbb{F}_q[t]$ in K following an idea of Gras [5].

Let q be a power of a prime number p. Let $k = \mathbb{F}_q(t)$ be the rational function field with constant field $\mathbb{F}_q$. Assume that the polynomial $T^p - T - D \in k[T]$ is irreducible. Let $K = k(\alpha)$ with $\alpha^p - \alpha = D$.

* Corresponding author.
E-mail addresses: hus04@mails.tsinghua.edu.cn (S. Hu), liyan_00@mails.tsinghua.edu.cn (Y. Li).

1071-5797/$ – see front matter
doi:10.1016/j.ffa.2010.03.004

Then K is called an Artin–Schreier extension of k (see [6]). It is well known that every cyclic extension of $\mathbb{F}_q(t)$ of degree p is an Artin–Schreier extension. In this paper, we explicitly describe the genus field of K. Using this result we also study the p-part of the ideal class group of the integral closure of $\mathbb{F}_q[t]$ in K. Our results combined with Peng's and Wittmann's results [8,13] give the complete results for genus theory of cyclic extensions of prime degree over rational function fields.

Let O_K be the integral closure of $\mathbb{F}_q[t]$ in K. Let $Cl(K)$ be the ideal class group of the Dedekind domain O_K. Let $G(K)$ be the genus field of K. Our paper is organized as follows. In Section 2, we recall the arithmetic of Artin–Schreier extensions. In Section 3, we recall the definition of $G(K)$ and compute the ambiguous ideal classes of $Cl(K)$ using cohomological methods. As a corollary, we obtain the order of $Gal(G(K)/K)$. In Section 4, we describe explicitly $G(K)$. In Section 5, we study the p-part of $Cl(K)$. We also give an analogue of the Rédei–Reichardt formula [11] for K.

2. The arithmetic of Artin–Schreier extensions

Let q be a power of a prime number p. Let $k=\mathbb{F}_q(t)$ be the rational function field. Let K/k be a cyclic extension of degree p. Then K/k is an Artin–Schreier extension, that is, $K=k(\alpha)$, where $\alpha^p-\alpha=D$, $D\in\mathbb{F}_q(t)$ and that D cannot be written as x^p-x for any $x\in k$. Conversely, for any $D\in\mathbb{F}_q(t)$ and D cannot be written as x^p-x for any $x\in k$, $k(\alpha)/k$ is a cyclic extension of degree p, where $\alpha^p-\alpha=D$. Two Artin–Schreier extensions $k(\alpha)$ and $k(\beta)$ such that $\alpha^p-\alpha=D$ and $\beta^p-\beta=D'$ are equal if and only if they satisfy the following relations,

$$\begin{aligned}
&\alpha \longrightarrow x\alpha+B_0=\beta,\\
&D \longrightarrow xD+\left(B_0^p-B_0\right)=D',\\
&x\in\mathbb{F}_p^*,\ B_0\in k.
\end{aligned}$$

(See [6] or Artin [2, pp. 180–181 and pp. 203–206].) Thus we can normalize D to satisfy the following conditions,

$$D=\sum_{i=1}^{m}\frac{Q_i}{P_i^{e_i}}+f(t),$$
$$(P_i,Q_i)=1,\quad\text{and}\quad p\nmid e_i,\quad\text{for } 1\leqslant i\leqslant m,$$
$$p\nmid\deg\bigl(f(t)\bigr),\quad\text{if } f(t)\notin\mathbb{F}_q,$$

where P_i $(1\leqslant i\leqslant m)$ are monic irreducible polynomials in $\mathbb{F}_q[t]$ and Q_i $(1\leqslant i\leqslant m)$ are polynomials in $\mathbb{F}_q[t]$ such that $\deg(Q_i)<\deg(P_i^{e_i})$. In the rest of this paper, we always assume D has the above normalized forms and denote $\frac{Q_i}{P_i^{e_i}}=D_i$, for $1\leqslant i\leqslant m$. The infinite place $(1/t)$ is split, inert, or ramified in K respectively when $f(t)=0$; $f(t)$ is a constant and the equation $x^p-x=f(t)$ has no solutions in $\mathbb{F}_q$; $f(t)$ is not a constant. Then the field K is called real, inert imaginary, or ramified imaginary, respectively. The finite places of k which are ramified in K are $P_1,\dots,P_m$ (see [6, p. 39]). Let $\mathfrak{P}_i$ be the place of K lying above P_i $(1\leqslant i\leqslant m)$.

Let P be a finite place of k which is unramified in K. Let $(P,K/k)$ be the Artin symbol at P. Then

$$(P,K/k)\alpha=\alpha+\left\{\frac{D}{P}\right\}$$

and the Hasse symbol $\{\frac{D}{P}\}$ is determined by the following equalities:

$$\begin{aligned}\left\{\frac{D}{P}\right\} &\equiv D + D^p + \cdots + D^{N(P)/p} \bmod P\\ &\equiv \left(D + D^q + \cdots + D^{N(P)/q}\right)\\ &\quad + \left(D + D^q + \cdots + D^{N(P)/q}\right)^p\\ &\quad + \cdots\\ &\quad + \left(D + D^q + \cdots + D^{N(P)/q}\right)^{q/p} \bmod P,\\ \left\{\frac{D}{P}\right\} &= \mathrm{tr}_{\mathbb{F}_q/\mathbb{F}_p}\, \mathrm{tr}_{(O_K/P)/\mathbb{F}_q}(D \bmod P)\end{aligned}$$

(see [6, p. 40]).

3. Ambiguous ideal classes

From this point on, we will use the following notations:

q	power of a prime number p.
k	the rational function field $\mathbb{F}_q(t)$.
K	a Galois extension of k.
G	the Galois group $Gal(K/k)$.
S	the set of infinite places of K (i.e, the primes above $(1/t)$).
O_K	the integral closure of $\mathbb{F}_q[t]$ in K.
$I(K)$	the group of fractional ideals of O_K.
$P(K)$	the group of principal fractional ideals of O_K.
$P(k)$	the subgroup of $P(K)$ generated by nonzero elements of $\mathbb{F}_q(t)$.
$Cl(K)$	the ideal class group of O_K.
$H(K)$	the Hilbert class field of K.
$G(K)$	the genus field of K.
U_K	the unit group of O_K.

Definition 3.1. (See Rosen [9].) The Hilbert class field $H(K)$ of K (relative to S) is the maximal unramified abelian extension of K such that all infinite places (i.e. $\in S$) of K split completely in $H(K)$.

Definition 3.2. (See Bae and Koo [3].) The genus field $G(K)$ of K is the maximal abelian extension of K in $H(K)$ which is the composite of K and some abelian extension of k.

For any G-module M, let M^G be the set of elements of M fixed by the action of G.

Definition 3.3. The ideal classes in $Cl(K)^G$ are called ambiguous ideal classes. The ideals in $I(K)^G$ are called ambiguous ideals.

The definition does not a priori imply that an ambiguous ideal class contains an ambiguous ideal. However, it turns out that in the setting of the paper, i.e. K/k is an Artin–Schreier extension, this is always the case. See Theorem 3.4 below. On the other hand, in more general situations, for example:

when K/k is a quadratic extension of odd characteristic, there can be ambiguous ideal classes that do not contain any ambiguous ideals. See Zhang [14] or Peng [8].

In the rest of this paper, we assume that K/k is an Artin–Schreier extension and σ is a fixed generator of G. Without loss of generality, we also assume that the extension K/k is geometric, i.e. the full constant field of K is $\mathbb{F}_q$ (see [10, p. 77]).

Theorem 3.4. *The ambiguous ideal classes of $Cl(K)$ form a vector space over $\mathbb{F}_p$ generated by $[\mathfrak{P}_1], [\mathfrak{P}_2], \ldots, [\mathfrak{P}_m]$ with dimension*

$$\dim_{\mathbb{F}_p} Cl(K)^G = \begin{cases} m-1, & \text{if } K \text{ is real}, \\ m, & \text{if } K \text{ is imaginary}. \end{cases}$$

Before the proof of the above theorem, we need some lemmas.

Lemma 3.5. $H^1(G, P(K)) = 1$.

Proof. From the following exact sequence

$$1 \longrightarrow U_K \longrightarrow K^* \longrightarrow P(K) \longrightarrow 1,$$

we have

$$1 \longrightarrow H^1\big(G, P(K)\big) \longrightarrow H^2(G, U_K) \longrightarrow H^2\big(G, K^*\big) \longrightarrow \cdots.$$

This is because $H^1(G, K^*) = 1$ (Hilbert Theorem 90). Since K/k is a cyclic extension, we have

$$H^2(G, U_K) \cong \hat{H}^0(G, U_K) = \frac{U_K^G}{NU_K} = \frac{\mathbb{F}_q^*}{(\mathbb{F}_q^*)^p} = 1. \tag{3.1}$$

So $H^1(G, P(K)) = 1$. $\square$

Lemma 3.6. *If K is imaginary, then $H^1(G, U_K) = 1$.*

Proof. Since K is imaginary, from Dirichlet unit theorem (see [10, p. 243]), we have $U_K = \mathbb{F}_q^*$. So

$$H^1\big(G, \mathbb{F}_q^*\big) = \frac{\{x \in \mathbb{F}_q^* \mid x^p = 1\}}{\{x^{\sigma-1} \mid x \in \mathbb{F}_q^*\}} = 1. \qquad \square$$

Lemma 3.7. *If K is real, then $H^1(G, U_K) \cong \mathbb{F}_p$.*

Proof. We denote by $\mathscr{D}$ the group of divisors of K, by $\mathscr{P}$ the subgroup of principal divisors. We define $\mathscr{D}(S)$ to be the subgroup of $\mathscr{D}$ generated by the primes in S and $\mathscr{D}^0(S)$ to be the degree zero divisors of $\mathscr{D}(S)$. From Proposition 14.1 of [10], we have the following exact sequence

$$1 \longrightarrow \mathbb{F}_q^* \longrightarrow U_K \longrightarrow \mathscr{D}^0(S) \longrightarrow Reg \longrightarrow 1,$$

where the map from U_K to $\mathscr{D}^0(S)$ is given by taking an element of U_K to its divisor and *Reg* is a finite group (see Proposition 14.1 and Lemma 14.3 of [10]). By Propositions 7 and 8 of [12, p. 134], we have

$h(U_K) = h(\mathscr{D}^0(S))$, where $h(*)$ is the Herbrand Quotient of $*$. By Eq. (3.1), we have $H^2(G, U_K) = 1$. Thus, we can prove this lemma by showing $h(\mathscr{D}^0(S)) = 1/p$.

Let ∞_1 be any infinite place in S. Thus $\mathscr{D}^0(S)$ is the free abelian group generated by $(\sigma - 1)\infty_1, (\sigma^2 - \sigma)\infty_1, \ldots, (\sigma^{p-1} - \sigma^{p-2})\infty_1$. And we have

$$\mathscr{D}^0(S) = \mathbb{Z}[G](\sigma - 1)\infty_1 \cong \frac{\mathbb{Z}[G]}{(1 + \sigma + \cdots + \sigma^{p-1})}. \tag{3.2}$$

Let ζ_p be a p-th primitive root of unity. We have

$$\frac{\mathbb{Z}[G]}{(1 + \sigma + \cdots + \sigma^{p-1})} \cong \mathbb{Z}[\zeta_p], \tag{3.3}$$

and the above map is given by taking σ to ζ_p. From (3.2) and (3.3), we have

$$H^1\big(G, \mathscr{D}^0(S)\big) = \frac{\ker N\mathscr{D}^0(S)}{(\sigma - 1)\mathscr{D}^0(S)} = \frac{\mathscr{D}^0(S)}{(\sigma - 1)\mathscr{D}^0(S)}$$
$$\cong \frac{\frac{\mathbb{Z}[G]}{(1+\sigma+\cdots+\sigma^{p-1})}}{(\sigma - 1)\frac{\mathbb{Z}[G]}{(1+\sigma+\cdots+\sigma^{p-1})}} \cong \frac{\mathbb{Z}[\zeta_p]}{(\zeta_p - 1)} \cong \mathbb{F}_p$$

and

$$H^2\big(G, \mathscr{D}^0(S)\big) = \frac{\mathscr{D}^0(S)^G}{N\mathscr{D}^0(S)} = 0.$$

Thus $h(\mathscr{D}^0(S)) = 1/p$. □

Proof of Theorem 3.4. From the following exact sequence

$$1 \longrightarrow P(K) \longrightarrow I(K) \longrightarrow Cl(K) \longrightarrow 1,$$

we have

$$1 \longrightarrow P(K)^G \longrightarrow I(K)^G \longrightarrow Cl(K)^G \longrightarrow H^1\big(G, P(K)\big) \longrightarrow \cdots.$$

Since $H^1(G, P(K)) = 1$ by Lemma 3.5, we have

$$1 \longrightarrow P(K)^G \longrightarrow I(K)^G \longrightarrow Cl(K)^G \longrightarrow 1.$$

Thus

$$1 \longrightarrow \frac{P(K)^G}{P(k)} \longrightarrow \frac{I(K)^G}{P(k)} \longrightarrow Cl(K)^G \longrightarrow 1. \tag{3.4}$$

From the following exact sequence

$$1 \longrightarrow U_K \longrightarrow K^* \longrightarrow P(K) \longrightarrow 1,$$

we have

$$1 \longrightarrow \mathbb{F}_q^* \longrightarrow k^* \longrightarrow P(K)^G \longrightarrow H^1(G, U_K) \longrightarrow 1$$

and

$$H^1(G, U_K) \cong \frac{P(K)^G}{P(k)}. \tag{3.5}$$

Since $\frac{I(K)^G}{P(k)}$ is a vector space over $\mathbb{F}_p$ with basis $[\mathfrak{P}_1], [\mathfrak{P}_2], \ldots, [\mathfrak{P}_m]$, by (3.4), (3.5), Lemmas 3.6 and 3.7, we get the desired result. □

Remark 3.8. If K is real, it is an interesting question to find explicitly the relation satisfied by $[\mathfrak{P}_1]$, $[\mathfrak{P}_2], \ldots, [\mathfrak{P}_m]$ in $Cl(K)^G$. By Lemma 3.5, if we can find a nontrivial element $\bar{u}$ of $H^1(G, U_K)$, then by Hilbert 90, we have $u = x^{\sigma-1}$, where $u \in U_K$ and $x \in K$. It is easy to see that

$$\sum_{i=1}^{m} \mathrm{ord}_{\mathfrak{P}_i}(x)[\mathfrak{P}_i] = 0$$

in $Cl(K)^G$.

From Proposition 2.4 of [3], we have

$$Gal\big(G(K)/K\big) \cong Cl(K)/Cl(K)^{(\sigma-1)} \cong Cl(K)^G. \tag{3.6}$$

(For the meaning of $Cl(K)^{(\sigma-1)}$, see the beginning of Section 5. It should be noted that the last isomorphism is merely an isomorphism of abelian groups but not canonical.) Therefore, we get:

Corollary 3.9.

$$\# Gal\big(G(K)/K\big) = \begin{cases} p^{m-1}, & \text{if } K \text{ is real}, \\ p^m, & \text{if } K \text{ is imaginary}. \end{cases}$$

Remark 3.10. One of referees told us that Corollary 3.9 is already contained in a paper by B. Angles (see [1, p. 269]). By the way, the same paper also points out an interesting fact that if m, i.e. the number of ramified places, is big enough then the Hilbert p-class field tower of K is infinite.

4. The genus field $G(K)$

In this section, we prove the following theorem which is the main result of this paper.

Theorem 4.1.

$$G(K) = \begin{cases} k(\alpha_1, \alpha_2, \ldots, \alpha_m), & \text{if } K \text{ is real}, \\ k(\beta, \alpha_1, \alpha_2, \ldots, \alpha_m), & \text{if } K \text{ is imaginary}, \end{cases}$$

where $\alpha_i^p - \alpha_i = D_i = \frac{Q_i}{P_i^{e_i}}$ $(1 \leqslant i \leqslant m)$, $\beta^p - \beta = f(t)$, *and* D_i, Q_i, P_i, $f(t)$ *are defined in Section* 2.

We only prove the imaginary case. The proof is similar for the real case. Since

$$\left(\sum_{i=1}^{m}\alpha_i+\beta\right)^p-\left(\sum_{i=1}^{m}\alpha_i+\beta\right)=\sum_{i=1}^{m}\frac{Q_i}{P_i^{e_i}}+f(t)=D,$$

we can assume $\alpha=\sum_{i=1}^{m}\alpha_i+\beta$. In order to prove the above theorem, we need two lemmas.

Lemma 4.2. *$E=k(\beta,\alpha_1,\alpha_2,\ldots,\alpha_m)$ is an unramified abelian extension of K.*

Proof. Let P be a place of k and let $(1/t)$ be the infinite place of k. If $P\neq P_1,P_2,\ldots,P_m,(1/t)$, then P is unramified in $k(\beta),k(\alpha_i)$ $(1\leqslant i\leqslant m)$, hence the places above P are unramified in E/K. Otherwise, without loss of generality, we can suppose $P=P_1$. Since $\alpha=\sum_{i=1}^{m}\alpha_i+\beta$, we have $E=Kk(\alpha_2,\ldots,\alpha_m,\beta)$. Thus $P=P_1$ is unramified in $k(\alpha_2,\ldots,\alpha_m,\beta)$, hence the place above P is unramified in E/K. □

Lemma 4.3. *The infinite places of K split completely in $E=k(\beta,\alpha_1,\alpha_2,\ldots,\alpha_m)$.*

Proof. Since $\alpha=\sum_{i=1}^{m}\alpha_i+\beta$, we have $E=Kk(\alpha_1,\alpha_2,\ldots,\alpha_m)$. Since the infinite place $(1/t)$ of k splits completely in $k(\alpha_1,\alpha_2,\ldots,\alpha_m)$, hence the place above $(1/t)$ also splits completely in E/K. □

Proof of Theorem 4.1. From Lemmas 4.2 and 4.3, we have

$$k(\alpha_1,\alpha_2,\ldots,\alpha_m,\beta)\subset G(K). \tag{4.1}$$

Comparing ramifications, $k(\beta),k(\alpha_i)$ $(1\leqslant i\leqslant m)$ are linearly disjoint over k, so

$$\big[k(\alpha_1,\alpha_2,\ldots,\alpha_m,\beta):k\big]=p^{m+1}$$

and

$$\big[k(\alpha_1,\alpha_2,\ldots,\alpha_m,\beta):K\big]=p^{m}.$$

Thus from Corollary 3.9 and (4.1), we get the result. □

5. The p-part of $Cl(K)$

Let l be a prime number and $\mathbb{Z}_l$ be the ring of l-adic integers. If K is a cyclic extension of k of degree l, then $Cl(K)_l$ is a finite module over the discrete valuation ring $\mathbb{Z}_l[\sigma]/(1+\sigma+\cdots+\sigma^{l-1})$ and $Cl(K)$ is a finite module over ring $\mathbb{Z}[\sigma]/(1+\sigma+\cdots+\sigma^{l-1})$. Denote the image of $(\sigma-1)^i$ acting on $Cl(K)_l$ and $Cl(K)$ by $Cl(K)_l^{(\sigma-1)^i}$ and $Cl(K)^{(\sigma-1)^i}$, respectively. The Galois module structure of $Cl(K)_l$ is determined by the dimensions:

$$\lambda_i=\dim\big(Cl(K)_l^{(\sigma-1)^{i-1}}/Cl(K)_l^{(\sigma-1)^i}\big)$$

for $i\geqslant 1$, these quotients being $\mathbb{F}_l$ vector spaces in a natural way. Since $\mathbb{Z}[\sigma]/(1+\sigma+\cdots+\sigma^{l-1})\cong\mathbb{Z}[\zeta_l]$ and $\prod_{i=1}^{l-1}(1-\zeta_l^i)=l$, the action of $\sigma-1$ on the non-l parts of $Cl(K)$ is invertible. So λ_i also equals to

$$\dim\big(Cl(K)^{(\sigma-1)^{i-1}}/Cl(K)^{(\sigma-1)^i}\big).$$

In number field situations, the dimensions λ_i have been investigated by Rédei [11] for $l = 2$ and Gras [5] for arbitrary l. In function field situations, these dimensions λ_i have been investigated by Wittmann for $l \neq p$. In this section, we give a formula to compute λ_2 for $l = p$. This is an analogue of the Rédei–Reichardt formula [11] for Artin–Schreier extensions.

If K is imaginary, as in the proof of Theorem 4.1, we suppose that $K = k(\alpha)$, where $\alpha = \sum_{i=1}^m \alpha_i + \beta$. We have the following sequence of maps

$$\begin{aligned} Cl(K)^G \longrightarrow Cl(K)/Cl(K)^{(\sigma-1)} &\cong Gal\big(G(K)/K\big) \hookrightarrow Gal\big(G(K)/k\big) \\ &\cong Gal\big(k(\alpha_1)/k\big) \times \cdots \times Gal\big(k(\alpha_m)/k\big) \times Gal\big(k(\beta)/k\big). \end{aligned}$$

Considering $[\mathfrak{P}_i] \in Cl(K)^G$ $(1 \leqslant i \leqslant m)$ under these maps, we have

$$\begin{aligned} [\mathfrak{P}_i] \longmapsto [\bar{\mathfrak{P}}_i] \longmapsto \big(\mathfrak{P}_i, G(K)/K\big) \longmapsto \big(\mathfrak{P}_i, G(K)/K\big) \\ \longmapsto \big(\big(P_i, k(\alpha_1)/k\big), \ldots, \big(P_i, k(\alpha_m)/k\big), \big(P_i, k(\beta)/k\big)\big), \end{aligned}$$

where the i-th component is $(\mathfrak{P}_i, G(K)/K)|_{k(\alpha_i)}$.

We define the Rédei matrix $R = (R_{ij}) \in M_{m\times m}(\mathbb{F}_p)$ as follows:

$$R_{ij} = \left\{\frac{D_j}{P_i}\right\}, \quad \text{for } 1 \leqslant i, j \leqslant m,\ i \neq j,$$

and R_{ii} is defined to satisfy the equality:

$$\sum_{j=1}^m R_{ij} + \left\{\frac{f}{P_i}\right\} = 0.$$

From the discussions in Section 2, we have

$$\begin{aligned} &\big(\mathfrak{P}_i, G(K)/K\big)\alpha = \alpha, \\ &\big(\mathfrak{P}_i, G(K)/K\big)\alpha_j = \alpha_j + \left\{\frac{D_j}{P_i}\right\}, \quad \text{for } i \neq j, \\ &\big(\mathfrak{P}_i, G(K)/K\big)\beta = \beta + \left\{\frac{f}{P_i}\right\}, \end{aligned}$$

so

$$\big(\mathfrak{P}_i, G(K)/K\big)\alpha_j = \alpha_j + R_{ij}, \quad \forall 1 \leqslant i, j \leqslant m.$$

Therefore it is easy to see that the image of $Cl(K)^G \to Cl(K)/Cl(K)^{(\sigma-1)}$ is isomorphic to the vector space spanned by the row vectors $(R_{i1}, R_{i2}, \ldots, R_{im}, \{\frac{f}{P_i}\})$ $(1 \leqslant i \leqslant m)$.

We conclude that

$$\begin{aligned} \lambda_2 &= \dim_{\mathbb{F}_p}\big(Cl(K)_p^{(\sigma-1)}/Cl(K)_p^{(\sigma-1)^2}\big) \\ &= \dim_{\mathbb{F}_p} \ker\big(Cl(K)_p^G \longrightarrow Cl(K)_p/Cl(K)_p^{(\sigma-1)}\big) \\ &= \dim_{\mathbb{F}_p} \ker\big(Cl(K)^G \longrightarrow Cl(K)/Cl(K)^{(\sigma-1)}\big) \end{aligned}$$

$$= \dim_{\mathbb{F}_p} Cl(K)^G - \dim_{\mathbb{F}_p} \mathrm{Im}\big(Cl(K)^G \longrightarrow Cl(K)/Cl(K)^{(\sigma-1)}\big)$$
$$= m - \mathrm{rank}(R).$$

Since the proof of the real case is similar, we only give the results and sketch the proof.

If K is real, from the discussions in Section 2, we have $f(t) = 0$, so

$$D = \sum_{i=1}^{m} D_i.$$

We define the Rédei matrix $R = (R_{ij}) \in M_{m\times m}(\mathbb{F}_p)$ as follows:

$$R_{ij} = \left\{\frac{D_j}{P_i}\right\}, \quad \text{for } 1 \leqslant i, j \leqslant m,\ i \neq j,$$

and R_{ii} is defined to satisfy the equality:

$$\sum_{j=1}^{m} R_{ij} = 0.$$

The same procedure as in the imaginary case shows that the image of $Cl(K)^G \to Cl(K)/Cl(K)^{(\sigma-1)}$ is isomorphic to the vector space spanned by the row vectors of the Rédei matrix. Thus

$$\lambda_2 = \dim_{\mathbb{F}_p} Cl(K)^G - \dim_{\mathbb{F}_p} \mathrm{Im}\big(Cl(K)^G \longrightarrow Cl(K)/Cl(K)^{(\sigma-1)}\big)$$
$$= m - 1 - \mathrm{rank}(R).$$

Theorem 5.1. *If K is imaginary, then $\lambda_2 = m - \mathrm{rank}(R)$; if K is real, then $\lambda_2 = m - 1 - \mathrm{rank}(R)$, where R is the Rédei matrix defined above.*

If $p = 2$, then σ acts as -1 on $Cl(K)$. So λ_1, λ_2 are equal to the 2-rank, 4-rank of the ideal class group $Cl(K)$, respectively. In particular, the above theorem tells us the 4-rank of the ideal class group $Cl(K)$ which is an analogue of the classical Rédei–Reichardt 4-rank formula for narrow ideal class groups of quadratic number fields.

Acknowledgments

The authors are enormously grateful to the two anonymous referees whose comments and suggestions lead to a large improvement of the paper.

References

[1] B. Angles, On the Hilbert class field tower of global function fields, Drinfeld modules, modular schemes and applications, in: E.-U. Gekeler, M. van der Put, M. Reversat, J. Van Geel (Eds.), Proceedings of the Workshop Held at Alden–Biesen, World Scientific, 1997.
[2] E. Artin, Algebraic Numbers and Algebraic Functions, AMS Chelsea Publishing, 2005.
[3] S. Bae, J.K. Koo, Genus theory for function fields, J. Aust. Math. Soc. Ser. A 60 (1996) 301–310.
[4] A. Fröhlich, Central Extensions, Galois Groups, and Ideal Classes of Number Fields, Contemp. Math., vol. 24, Amer. Math. Soc., Providence, 1983.
[5] G. Gras, Sur les l-classes d'idéaux dans les extensions cycliques relatives de degré premier l, I, II, Ann. Inst. Fourier (Grenoble) 23 (3) (1973) 1–48, Ann. Inst. Fourier (Grenoble) 23 (4) (1973) 45–64.
[6] H. Hasse, Theorie der relativ-zyklischen algebraischen Funktionenkörper, insbesondere bei endlichem Konstantenkörper, J. Reine Angew. Math. 172 (1934) 37–54.

[7] H. Hasse, Zur Geschlechtertheorie in quadratischen Zahlkörpern, J. Math. Soc. Japan 3 (1951) 45–51.
[8] G. Peng, The genus fields of Kummer function fields, J. Number Theory 98 (2003) 221–227.
[9] M. Rosen, The Hilbert class field in function fields, Expo. Math. 5 (1987) 365–378.
[10] M. Rosen, Number Theory in Function Fields, Springer-Verlag, New York, 2002.
[11] L. Rédei, Arithmetischer Beweis des Satzes über die Anzahl der durch vier teilbaren Invarianten der absoluten Klassengruppe im quadratischen Zahlkörper, J. Reine Angew. Math. 171 (1935) 55–60.
[12] J.P. Serre, Local Fields, Springer-Verlag, New York, 1979.
[13] C. Wittmann, *l*-Class groups of cyclic function fields of degree *l*, Finite Fields Appl. 13 (2007) 327–347.
[14] X. Zhang, Ambiguous classes and 2-ranks of class groups of quadratic function fields, J. China Univ. Sci. Tech. 17 (1987) 425–430.