Canad. J. Math. 2023, pp. 1–22
http://dx.doi.org/10.4153/S0008414X23000652

Infinite families of Artin–Schreier function fields with any prescribed class group rank

Jinjoo Yoo and Yoonjin Lee

Abstract. We study the Galois module structure of the class groups of the Artin–Schreier extensions K over k of extension degree p, where $k := \mathbb{F}_q(T)$ is the rational function field and p is a prime number. The structure of the p-part $Cl_K(p)$ of the ideal class group of K as a finite G-module is determined by the invariant λ_n, where $G := \mathrm{Gal}(K/k) = \langle\sigma\rangle$ is the Galois group of K over k, and $\lambda_n = \dim_{\mathbb{F}_p}(Cl_K(p)^{(\sigma-1)^{n-1}}/Cl_K(p)^{(\sigma-1)^n})$. We find infinite families of the Artin–Schreier extensions over k whose ideal class groups have guaranteed prescribed λ_n-rank for $1 \le n \le 3$. We find an algorithm for computing λ_3-rank of $Cl_K(p)$. Using this algorithm, for a given integer $t \ge 2$, we get infinite families of the Artin–Schreier extensions over k whose λ_1-rank is t, λ_2-rank is $t-1$, and λ_3-rank is $t-2$. In particular, in the case where $p = 2$, for a given positive integer $t \ge 2$, we obtain an infinite family of the Artin–Schreier quadratic extensions over k whose 2-class group rank (resp. 2^2-class group rank and 2^3-class group rank) is *exactly* t (resp. $t-1$ and $t-2$). Furthermore, we also obtain a similar result on the 2^n-ranks of the divisor class groups of the Artin–Schreier quadratic extensions over k.

1 Introduction

There have been active studies on the structure of the class groups of number fields and function fields; for instance, we refer to [1–5, 6, 8, 10, 11, 13–16, 19–25]. For studying the structure of class groups, the following methods have been used: *genus theory* [1, 3, 6], *Rédei matrix* [2, 15, 23], and *Conner and Hurrelbrink's exact hexagon* [5, 13].

The Galois module structure of the class groups of cyclic extensions over the rational function field $k := \mathbb{F}_q(T)$ has been studied in [2, 8, 14, 19], where $\mathbb{F}_q$ is a finite field of order q. We need to introduce the following definitions for description of the previous developments. Let K be a cyclic extension over k of extension degree prime p. We denote the *ideal class group* of K by Cl_K and that of *divisor class group* by J_K. Let $G := \mathrm{Gal}(K/k)$ be the Galois group of K over k. Then Cl_K and J_K are finite G-modules. Let σ be a generator of G and $\mathbb{Z}_p$ the ring of p-adic integer. The

Received by the editors October 15, 2022; revised September 9, 2023; accepted October 9, 2023.
Published online on Cambridge Core October 19, 2023.
J. Yoo is supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (Grant Nos. MSIT-2020R1A4A1016649 and MEST-2022R1A2C1009297), and also by the Basic Science Research Program through the NRF funded by the Ministry of Education (Grant No. 2021R1I1A1A01047765). Y. Lee is supported by the Basic Science Research Program through the NRF funded by the Ministry of Education (Grant No. 2019R1A6A1A11051177) and the NRF grant funded by the Korea government (MEST) (Grant No. NRF-2022R1A2C1003203).
AMS subject classification: **11R29, 11R58.**
Keywords: Artin–Schreier extension, function field, class group, ideal class group, Galois module.

structures of $Cl_K(p)$ and $J_K(p)$ as finite modules over the discrete valuation ring $\mathbb{Z}_p[\sigma]/(1+\sigma+\cdots+\sigma^{p-1}) \simeq \mathbb{Z}_p[\zeta_p]$ are determined by the following ranks:

$$\lambda_n := \dim_{\mathbb{F}_p}(Cl_K(p)^{(\sigma-1)^{n-1}}/Cl_K(p)^{(\sigma-1)^n}) \quad \text{and}$$
$$\mu_n := \dim_{\mathbb{F}_p}(J_K(p)^{(\sigma-1)^{n-1}}/J_K(p)^{(\sigma-1)^n}),$$

where $Cl_K(p)$ (resp. $J_K(p)$) is the p-Sylow subgroup of Cl_K (resp. J_K) and ζ_p is a primitive pth root of unity.

We point out that in particular, when $p = 2$, the rank λ_n of Cl_K is exactly equal to the 2^n-rank of Cl_K and the rank μ_n of J_K gives the 2^n-rank of J_K, where the 2^n-rank of Cl_K is defined as $\dim_{\mathbb{F}_2}(Cl_K^{2^{n-1}}/Cl_K^{2^n})$ and similarly for J_K. This is because σ acts -1 on Cl_K, which implies that the rank λ_n of the finite module Cl_K over $\mathbb{Z}[\zeta_2] = \mathbb{Z}$ is exactly the 2^n-rank of Cl_K, and similarly it also holds for J_K.

There are exactly two kinds of cyclic extensions of prime extension degree over the rational function field k: *Kummer extension* and *Artin–Schreier extension*. For Kummer extensions L over k, Anglés and Jaulent [1] (resp. Wittmann [19]) studied the λ_1-rank (resp. λ_2-rank) of the ideal class groups of L and the authors of this paper [22] studied the λ_3-rank of the ideal class groups of L. Furthermore, for Artin–Schreier extensions over k, there also have been some studies on the computation of λ_1 and λ_2 for their ideal class groups [2, 8]. However, there has been no result yet on finding infinite families of Artin–Schreier extensions over k whose ideal class groups have guaranteed prescribed λ_n-rank of the ideal class group of Artin–Schreier extension for $1 \le n \le 3$. This is one of the motivations of our paper.

In this paper, we study the Galois module structure of the class groups of the Artin–Schreier extensions K over k of extension degree p, where $k := \mathbb{F}_q(T)$ is the rational function field of characteristic p and p is a prime number. The structure of the p-part $Cl_K(p)$ of the ideal class group of K as a finite G-module is determined by the invariant λ_n, where $G := \mathrm{Gal}(K/k) = \langle\sigma\rangle$. In detail, first of all, for a given positive integer t, we obtain infinite families of K over k whose λ_1-rank of Cl_K is t and λ_n-rank of Cl_K is zero for $n \ge 2$, depending on the ramification behavior of the infinite place ∞ of k (Theorems 3.2–3.4). We then find infinite families of the Artin–Schreier extensions over k whose ideal class groups have guaranteed prescribed λ_n-rank for n up to 3. We find an algorithm for computing λ_3-rank of $Cl_K(p)$. Using this algorithm, for a given integer $t \ge 2$, we get infinite families of the Artin–Schreier extensions over k whose λ_1-rank is t, λ_2-rank is $t-1$, and λ_3-rank is $t-2$ (Theorem 5.1). In particular, in the case where $p = 2$, for a given positive integer $t \ge 2$, we obtain an infinite family of the Artin–Schreier quadratic extensions over k which have 2-class group rank *exactly* t, 2^2-class group rank $t-1$, and 2^3-class group rank $t-2$ (Corollary 5.3). Furthermore, we also obtain a similar result on the 2^n-ranks of the divisor class groups of the Artin–Schreier quadratic extensions over k for n up to 3 (Corollary 5.4). Finally, in Tables 1 and 2, we give some implementation results for explicit infinite families using Theorems 3.2–3.4 and 5.1. These implementation results are done by MAGMA.

We remark that as a main tool for computation of λ_3, we use an analogue of *Rédei matrix*. We emphasize that there is no number field analogue for the Artin–Schreier extensions over k, while there is a number field analogue for Kummer extensions over k.

https://doi.org/10.4153/S0008414X23000652 Published online by Cambridge University Press

2 Preliminaries

Let q be a power of a prime number p, and let $k := \mathbb{F}_q(T)$ be the *rational function field*. The prime divisor of k corresponding to $(1/T)$ is called the *infinite place* and denoted by ∞. Let K/k be a cyclic extension of degree p. Then K/k is an *Artin–Schreier extension*: that is, $K = k(\alpha)$, where $\alpha^p - \alpha = D$, $D \in k$, and that D cannot be written as $x^p - x$ for any $x \in k$. Conversely, for any $D \in k$ 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 $\alpha^p - \alpha = D$.

For $D, D' \in k$, let $K_1 := k(\alpha)$ and $K_2 := k(\beta)$ be two Artin–Schreier extensions over k with $\alpha^p - \alpha = D$ and $\beta^p - \beta = D'$, respectively. Two Artin–Schreier extensions K_1 and K_2 are equal if and only if they satisfy the following relations [8, p. 256]:

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

Thus, D can be *normalized* to satisfy the following conditions:

$$\begin{aligned} D &= \sum_{i=1}^{m} \frac{Q_i}{P_i^{r_i}} + f(T), \\ &(P_i, Q_i) = 1, \ p \nmid r_i \text{ for } 1 \le i \le t, \\ &p \nmid \deg f(T) \ \text{ if } \deg f(T) \ge 1, \text{ and} \\ &f(T) = 0 \ \text{ if } f(T) \in \mathbb{F}_q \text{ with } \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(f) = 0, \end{aligned} \tag{2.1}$$

where P_i is a monic irreducible polynomial in $\mathbb{F}_q[T]$, $Q_i, f(T) \in \mathbb{F}_q[T]$, and $\deg Q_i < \deg P_i^{r_i}$ for $1 \le i \le t$; the last condition follows from noting that if $f(T) = c$ in $\mathbb{F}_q^\times$ with $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(c) = 0$, then there exists $b \in \mathbb{F}_q^\times$ such that $b^p - b = c$.

Throughout this paper, let $K := k(\alpha_{D_m})$ be the Artin–Schreier extension over k of extension degree p, where $x^p - x = D_m$ has no root in k, α_{D_m} is a root of $x^p - x = D_m$, and the normalized D_m satisfies (2.1). We note that all the finite places of k which are totally ramified in K are $P_1, \ldots, P_t$. In the following lemma, we state the ramification behavior of the infinite place ∞ of k in K.

Lemma 2.1 [8, p. 256] *Let $K = k(\alpha_{D_m})$ be the Artin–Schreier extension over k of extension degree p, where $\alpha_{D_m}^p - \alpha_{D_m} = D_m$ and D_m is defined in (2.1). Then we have the followings.*

(i) *The infinite place ∞ of k is totally ramified in K if and only if* $\deg f(T) \ge 1$.
(ii) *The infinite place ∞ of k is inert in K if and only if $f(T) = c \in \mathbb{F}_q^\times$, where $x^p - x - c$ is irreducible over $\mathbb{F}_q$.*
(iii) *The infinite place ∞ of k splits completely in K if and only if $f(T) = 0$.*

For descriptions of λ_1 and λ_2, we use the notion of *the Hasse symbol* which is first introduced in [7].

Definition 2.1 [8, p. 257] Let $K = k(\alpha_{D_m})$ be the Artin–Schreier extension over k of extension degree p, where $\alpha_{D_m}^p - \alpha_{D_m} = D_m$ for some $D_m \in k$. Let P be a finite place of k which is unramified in K, and let $\left(\frac{K/k}{P}\right)$ be the *Artin symbol* of P. Then $\left(\frac{K/k}{P}\right)\alpha_{D_m} =$

https://doi.org/10.4153/S0008414X23000652 Published online by Cambridge University Press

$\alpha_{D_m} + \left\{\frac{D_m}{P}\right\}$, where $\left\{\frac{D_m}{P}\right\}$ is defined as follows:

$$\left\{\frac{D_m}{P}\right\} = \mathrm{Tr}_{(\mathcal{O}_K/P)/\mathbb{F}_p}(D_m \bmod P);$$

$\mathrm{Tr}_{(\mathcal{O}_K/P)/\mathbb{F}_p}$ denotes the *trace* function from $\mathcal{O}_K/P$ to $\mathbb{F}_p$ and $\mathcal{O}_K$ is the integral closure of K. We call $\left\{\frac{\cdot}{\cdot}\right\}$ *the Hasse symbol.*

Lemma 2.2 [8] *Let $K = k(\alpha_{D_m})$ be the Artin–Schreier extension over k of extension degree p, where $\alpha_{D_m}^p - \alpha_{D_m} = \sum_{i=1}^{m} \frac{Q_i}{P_i^{r_i}} + f(T)$, which is defined in (2.1). Then we have the followings.*

(i) $\lambda_1 = \begin{cases} m & \text{if } \deg f(T) \geq 1 \text{ or} \\ & \quad f(T) = c \in \mathbb{F}_q^\times, \text{ where } x^p - x = c \in \mathbb{F}_q^\times \text{ is irreducible over } \mathbb{F}_q, \\ m-1 & \text{if } f(T) = 0. \end{cases}$

(ii) *We have $\lambda_2 = \lambda_1 - \mathrm{rank}(R)$, where $R = [r_{ij}]$ is a matrix over $\mathbb{F}_p$ defined by*

$$r_{ij} = \begin{cases} \left\{\frac{Q_j/P_j^{r_j}}{P_i}\right\}, & \text{for } 1 \leq i \neq j \leq m, \\ -\left(\sum_{j=1, i\neq j}^{m} r_{ij} + \left\{\frac{f}{P_i}\right\}\right), & \text{for } 1 \leq i = j \leq m. \end{cases}$$

We call such matrix R as the Rédei matrix.

We recall that the *Hilbert class field* H_K of K is the maximal unramified abelian extension of K where the infinite places of k split completely in K. The *genus field* $\mathcal{G}_K$ *of* K is the maximal subextension $K \subseteq \mathcal{G}_K \subseteq H_K$ which is abelian over k. In Lemma 2.3, we state a description of the genus field of the Artin–Schreier extension.

Lemma 2.3 [8, Theorem 4.1] *Let $K = k(\alpha_{D_m})$ be the Artin–Schreier extension over k of extension degree p, where D_m is defined in (2.1) and α_{D_m} is a root of $x^p - x = D_m$. Let α_i (resp. β) be a root of $x^p - x = Q_i/P_i^{r_i}$ for $1 \leq i \leq m$ (resp. $x^p - x = f(T)$) in $\overline{k}$. Then the genus field $\mathcal{G}_K$ of K is $\mathcal{G}_K = k(\alpha_1, \ldots, \alpha_m, \beta)$.*

We now introduce explicit criteria for determining whether a place of k is totally ramified or not in the Artin–Schreier extension K.

Lemma 2.4 [18, Proposition 3.7.8] *Let $K = k(y)$ be the Artin–Schreier extension over k of extension degree p, where $y^p - y = u$ for some $u \in k$. For a place P of k, we define the integer m_P by*

$$m_P := \begin{cases} m, & \text{if there is an element } z \in k \text{ satisfying} \\ & v_P(u - (z^p - z)) = -m < 0 \text{ and } m \not\equiv 0 \pmod{p}, \\ -1, & \text{if } v_P(u - (z^p - z)) \geq 0 \text{ for some } z \in k. \end{cases}$$

Then we have the followings.

(i) *P is totally ramified in K/k if and only if $m_P > 0$.*
(ii) *P is unramified in K/k if and only if $m_P = -1$.*

Lemma 2.5 [17, Proposition 14.1] *Let K be a function field over the rational function field $k = \mathbb{F}_q(T)$, and let ∞ be the infinite place of k. Denote the ideal class group (resp.*

the divisor class group) of K by Cl_K (resp. J_K) and S be a set of places of K lying over ∞. Then

$$0 \to \mathcal{D}_K^0(S)/\mathcal{P}_K(S) \to J_K \to Cl_K \to \mathbb{Z}/d\mathbb{Z} \to 0$$

is an exact sequence, where $\mathcal{D}_K^0(S)$ is the divisor group with support only in S whose degree is zero, $\mathcal{P}_K(S)$ is a principal divisor with support only in S, and d is the greatest common divisor of the elements in $\{\deg P : P \in S\}$.

Using Lemma 2.5, we can easily obtain the following corollary, which gives relation between the ideal class group of K and the divisor class group of K, where K is the Artin–Schreier function field over k.

Lemma 2.6 *Let K be the Artin–Schreier extension over k with extension degree p, and let all the notations be the same as in Lemma 2.5. Then we have the following.*

(i) *If ∞ is totally ramified in K, then $\mathcal{D}_K^0(S)$ is trivial and $d = 1$; thus,*

$$0 \to J_K \to Cl_K \to 0$$

is exact.

(ii) *If ∞ is inert in K, then $\mathcal{D}_K^0(S)$ is trivial and $d = p$; therefore,*

$$0 \to J_K \to Cl_K \to \mathbb{Z}/p\mathbb{Z} \to 0$$

is an exact sequence.

(iii) *If ∞ splits completely in K, then $d = 1$; thus,*

$$0 \to \mathcal{D}_K^0(S)/\mathcal{P}_K(S) \to J_K \to Cl_K \to 0$$

is exact.

3 Infinite families of Artin–Schreier function fields with any prescribed class group λ-rank

In this section, for any positive integer t, we find infinite families of Artin–Schreier function fields K over k whose λ-rank of the ideal class group Cl_K of K is t and λ_n-rank of Cl_K is zero for $n \geq 2$, depending on the ramification behavior of the infinite place ∞ of k. Theorem 3.2 deals with the case where the infinite place ∞ of k is totally ramified in K and Theorem 3.3 (resp. Theorem 3.4) treats the case where the infinite place ∞ of k splits completely (resp. ∞ is inert) in K.

We first give the following lemma, which shows the property of the trace over finite fields. This lemma plays a key role in the proofs of Theorems 3.2–3.4.

Lemma 3.1 *Let h be a monic irreducible polynomial in $\mathbb{F}_q[T]$ and $\mathfrak{h} := q^{\deg h}$. Let g be a nonzero element in $\mathbb{F}_q[T]$, and let $\tilde{g} \in \mathbb{F}_{\mathfrak{h}}$ be $\phi \circ \pi(g)$, where*

$$g \in \mathbb{F}_q[T] \xrightarrow{\pi} \pi(g) \in \mathbb{F}_q[T]/\langle h \rangle \xrightarrow{\phi} \mathbb{F}_{\mathfrak{h}}.$$

Then we have $\mathrm{Tr}_{\mathbb{F}_{\mathfrak{h}}/\mathbb{F}_q} \widetilde{g} = 0$ *if and only if the following holds:*

(i) *If* $\deg g = 0$*, then* $q \mid \deg h$*.*
(ii) *If* $\deg g \geq 1$*, then* $g \equiv b(T)^q - b(T) \pmod{h}$ *for some* $b(T) \in \mathbb{F}_q[T]$*.*

Proof We note that $\mathbb{F}_{\mathfrak{h}} \simeq \mathbb{F}_q[T]/\langle h \rangle$ since h is an irreducible polynomial over $\mathbb{F}_q$.

First, assume that $\deg g = 0$: that is, g is an element of $\mathbb{F}_q^\times$, and so $g = \tilde{g}$. Then we have the following:

$$\mathrm{Tr}_{\mathbb{F}_{\mathfrak{h}}/\mathbb{F}_q} \tilde{g} = 0 \text{ if and only if } q \mid \deg h;$$

this is because $\mathrm{Tr}_{\mathbb{F}_{\mathfrak{h}}/\mathbb{F}_q} \tilde{g} = \tilde{g} \cdot \deg h$ in $\mathbb{F}_q$.

Now, we consider the case where $\deg g \geq 1$. Assume that $g \equiv b(T)^q - b(T) \pmod{h}$. Then we have

$$\tilde{g} = \phi \circ \pi(g) = \phi((b(T))^q - (b(T))) = \phi(b(T))^q - \phi(b(T)) = \tilde{b}^q - \tilde{b},$$

where $\tilde{b} := \phi(b(T)) \in \mathbb{F}_{\mathfrak{h}}$. Therefore, the result follows immediately by [12, Theorem 2.25]. Conversely, now assume that $\mathrm{Tr}_{\mathbb{F}_{\mathfrak{h}}/\mathbb{F}_q}(\tilde{g}) = 0$: that is, there exists some $\tilde{b} \in \mathbb{F}_{\mathfrak{h}}$ such that $\tilde{g} = \tilde{b}^q - \tilde{b}$. Let $b(T) := \phi^{-1}(\tilde{b})$; there exists such $b(T) \in \mathbb{F}_q[T]$ since ϕ is isomorphism. Thus, we get

$$g = \pi^{-1} \circ \phi^{-1}(\tilde{g}) = \pi^{-1} \circ \phi^{-1}(\tilde{b}^q - \tilde{b}) = \pi^{-1}((b(T))^q - (b(T)));$$

this implies that $g \equiv b(T)^q - b(T) \pmod{h}$. ∎

Theorem 3.2 *Let t be a positive integer. Let* $K = k(\alpha_{D_t})$ *be the Artin–Schreier extension over the rational function field* $k = \mathbb{F}_q(T)$ *of extension degree p, where*

$$\alpha_{D_t}^p - \alpha_{D_t} = \sum_{i=1}^{t} \frac{Q_i}{P_i^{r_i}} + f(T)$$

satisfies (2.1). Assume that the infinite place ∞ *of k is totally ramified in K; equivalently,* $\deg f(T) \geq 1$ *with* $p \nmid \deg f(T)$*. We further assume that the followings hold:*

(i) $p \nmid \deg P_i$ *for any i with* $1 \leq i \leq t$*.*
(ii) $f(T) \equiv \mathfrak{c}_i \pmod{P_i}$*, where* $\mathfrak{c}_i \in \mathbb{F}_q^\times$ *such that* $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\mathfrak{c}_i) \neq 0$ *for any i with* $1 \leq i \leq t$*.*
(iii) $Q_j \equiv P_j^{r_j}(b_i(T)^q - b_i(T)) \pmod{P_i}$ *for any i with* $1 \leq i \neq j \leq t$*, where* $b_i(T)$ *is a polynomial in* $\mathbb{F}_q[T]$*.*

Then the λ_1*-rank of the ideal class group* Cl_K *of K and* μ_1*-rank of the divisor class group* J_K *of K are t. Moreover, for* $n \geq 2$*, the* λ_n*-rank of* Cl_K *and the* μ_n*-rank of* J_K *are zero.*

In particular, for the case when $p = 2$*, the 2-class groups* $Cl_K(2)$ *and* $J_K(2)$ *are elementary abelian 2-groups: that is, isomorphic to* $(\mathbb{Z}/2\mathbb{Z})^t$*.*

Proof We note that by Lemma 2.6, the ideal class group of K and the divisor class group of K are isomorphic; thus, $\lambda_n = \mu_n$ for $n \geq 1$. Since λ_n is a decreasing sequence as n grows (λ_{n-1} and λ_n may have the same value), it suffices to show the following:

$$\lambda_1 = t \quad \text{and} \quad \lambda_2 = 0. \tag{3.1}$$

https://doi.org/10.4153/S0008414X23000652 Published online by Cambridge University Press

By Lemma 2.2, we can easily get $\lambda_1 = t$. Thus, we will show that the rank of R is t, where R is the Rédei matrix over $\mathbb{F}_p$ which is defined in Lemma 2.2.

Let $f(T)$ be a polynomial in $\mathbb{F}_q[T]$ which satisfies condition (ii). For convenience, let $\delta_i := \deg P_i$ for $1 \le i \le t$. Then we have the following:

$$\mathrm{Tr}_{\mathbb{F}_{q^{\delta_i}}/\mathbb{F}_q}(f \pmod{P_i}) = \mathrm{Tr}_{\mathbb{F}_{q^{\delta_i}}/\mathbb{F}_q} \mathfrak{c}_i = \delta_i \mathfrak{c}_i;$$

the last equality follows from the fact that $\mathfrak{c}_i \in \mathbb{F}_q^\times$. Thus, by the definition of the Hasse symbol, we obtain

(3.2)
$$\left\{\frac{f(T)}{P_i}\right\} = \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\mathrm{Tr}_{\mathbb{F}_{q^{\delta_i}}/\mathbb{F}_q}(f \pmod{P_i})) = \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\delta_i \mathfrak{c}_i) = \delta_i \,\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p} \mathfrak{c}_i \neq 0;$$

for the last equality, we use conditions (i) and (ii).

Now, let Q_j $(1 \le j \le t)$ be a polynomial in $\mathbb{F}_q[T]$ which satisfies condition (iii). Then, for $1 \le i \neq j \le t$, we have

$$Q_j \overline{P_j}^{r_j} \equiv b_i(T)^q - b_i(T) \pmod{P_i},$$

where $P_j \overline{P_j} \equiv 1 \pmod{P_i}$. We note that $\overline{P_j}$ always exist since P_i and P_j are relative prime in $\mathbb{F}_q[T]$. Then, by Lemma 3.1, we obtain $\mathrm{Tr}_{\mathbb{F}_{\delta_i}/\mathbb{F}_q}(Q_j \overline{P_j}^{r_j} \pmod{P_i}) = 0$, where $\delta_i := \deg P_i$. Thus, we obtain

$$\left\{\frac{Q_j/P_j^{r_j}}{P_i}\right\} = \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\mathrm{Tr}_{\mathbb{F}_{q^{\delta_i}}/\mathbb{F}_q}(Q_j \overline{P_j}^{r_j} \pmod{P_i}) = \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p} 0 = 0. \tag{3.3}$$

Therefore, we get a $t \times t$ Rédei matrix $R = [r_{ij}]$ over $\mathbb{F}_p$ as follows:

$$R = \begin{bmatrix} r_{11} & 0 & \cdots & 0 \\ 0 & r_{22} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & r_{tt} \end{bmatrix}, \tag{3.4}$$

where $r_{ii} = \left\{\frac{f(T)}{P_i}\right\} \neq 0$ in $\mathbb{F}_p$ for every $1 \le i \le t$. We can easily check that the rank of R is t; therefore, we get $\lambda_2 = \lambda_1 - \mathrm{rank}(R) = 0$.

For the case where $p = 2$, the 2^n-rank of Cl_K and that of J_K are exactly λ_n and μ_n, respectively; therefore, $Cl_K(2) \simeq J_K(2) \simeq (\mathbb{Z}/2\mathbb{Z})^t$. ∎

Theorem 3.3 *Let t be a positive integer. Let $K = k(\alpha_{D_{t+1}})$ be the Artin–Schreier extension over the rational function field $k = \mathbb{F}_q(T)$ of extension degree p, where*

$$\alpha_{D_{t+1}}^p - \alpha_{D_{t+1}} = \sum_{i=1}^{t+1} \frac{Q_i}{P_i^{r_i}} + f(T)$$

satisfies (2.1). Assume that the infinite place ∞ splits completely in K; equivalently, $f(T) = 0$. We further assume that the followings hold:

(i) *$p \nmid \deg P_i$ for any i with $1 \le i \le t+1$.*
(ii) *$Q_t \equiv \mathfrak{c}_i P_t^{r_t} \pmod{P_i}$, where $\mathfrak{c}_i \in \mathbb{F}_q^\times$ such that $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\mathfrak{c}_i) \neq 0$ for any i with $1 \le i \le t$.*

https://doi.org/10.4153/S0008414X23000652 Published online by Cambridge University Press

(iii) $Q_j \equiv P_j^{r_j}(b_i(T)^q - b_i(T)) \pmod{P_i}$ *for any* $1 \le i \le t+1$, $1 \le j \le t$, $i \ne j$, *where* $b_i(T) \in \mathbb{F}_q[T]$.

Then the λ_1*-rank of the ideal class group* Cl_K *of K is t. Moreover, for* $n \ge 2$, *the* λ_n*-rank of* Cl_K *is zero.*

In particular, for the case when $p = 2$, *the* 2*-class group* $Cl_K(2)$ *is an elementary abelian* 2*-group: that is, isomorphic to* $(\mathbb{Z}/2\mathbb{Z})^t$.

Proof As in Theorem 3.2, we will show (3.1). The fact that $\lambda_1 = t$ comes immediately from Lemma 2.2. Thus, it is sufficient to show that $\lambda_2 = 0$: that is, $\text{rank}(R) = \lambda_1 = t$, where R is the Rédei matrix of K defined in Lemma 2.2.

Let $D_i := \frac{Q_i}{P_i^{r_i}}$ for $1 \le i \le t+1$. Using the same reasoning as in Theorem 3.2, we get $\{D_t/P_i\} \ne 0$ for every $1 \le i \le t$; we note that we use conditions (i) and (ii). Thus, the $i(t+1)$th entry of R is nonzero for $1 \le i \le t$. By condition (iii), we obtain $\{D_j/P_i\} = 0$ from Lemma 3.1; this implies that the ijth entries of R are all zero for $1 \le i \le t+1$ and $1 \le j \le t$ with $i \ne j$.

Therefore, we obtain a $(t+1) \times (t+1)$ matrix $R = [r_{ij}]$ over $\mathbb{F}_p$ as follows:

$$R = \begin{bmatrix} -r_{1,t+1} & 0 & \cdots & 0 & r_{1,t+1} \\ 0 & -r_{2,t+1} & \cdots & 0 & r_{2,t+1} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & -r_{t,t+1} & r_{t,t+1} \\ 0 & 0 & \cdots & 0 & 0 \end{bmatrix},$$

where $r_{i,t+1} \ne 0$ in $\mathbb{F}_p$ for every $1 \le i \le t$. Thus, the result follows immediately.

For the case where $p = 2$, since λ_n gives the full 2^n-rank of Cl_K, we obtain that $Cl_K(2) \simeq (\mathbb{Z}/2\mathbb{Z})^t$. ∎

Theorem 3.4 *Let t be a positive integer. Let* $K = k(\alpha_{D_t})$ *be the Artin–Schreier extension over the rational function field* $k = \mathbb{F}_q(T)$ *of extension degree p, where*

$$\alpha_{D_t}^p - \alpha_{D_t} = \sum_{i=1}^{t} \frac{Q_i}{P_i^{r_i}} + f(T)$$

satisfies (2.1). Assume that ∞ *is inert in K; equivalently,* $f(T) = c \in \mathbb{F}_q^{\times}$, *where* $x^p - x - c$ *is irreducible over* $\mathbb{F}_q$. *We further assume that the followings hold: for some* $\mathfrak{c} \in \mathbb{F}_q$,

(i) $p \nmid \deg P_i$ *for every* $1 \le i \le t$.
(ii) $Q_j \equiv P_j^{r_j}(b_i(T)^q - b_i(T))$ *for any i with* $1 \le i \ne j \le t$, *where* $b_i(T) \in \mathbb{F}_q[T]$.

Then the λ_1*-rank of the ideal class group* Cl_K *of K is t. Moreover, for* $n \ge 2$, *the* λ_n*-rank of* Cl_K *is zero.*

In particular, for the case when $p = 2$, *then* $Cl_K(2)$ *is isomorphic to* $(\mathbb{Z}/2\mathbb{Z})^t$ *and* $J_K(2)$ *is isomorphic to* $(\mathbb{Z}/2\mathbb{Z})^{t-1}$.

Proof We can simply get $\lambda_1 = t$ by Lemma 2.2; we now show that $\lambda_2 = 0$, which implies that the rank of the Rédei matrix R is t. As usual, set $D_i := \frac{Q_i}{P_i^{r_i}}$. Using Lemma 3.1, we obtain $\{D_j/P_i\} = 0$ for every $1 \le i \ne j \le t$. Now, we compute $\{c/P_i\}$ for $1 \le i \le t$, where $c \in \mathbb{F}_q^{\times}$. Let δ_i be the degree of P_i. By the definition of Hasse norm, we have

$$\left\{\frac{c}{P_i}\right\} = \text{Tr}_{\mathbb{F}_q/\mathbb{F}_p} \text{Tr}_{\mathbb{F}_q^{\delta_i}/\mathbb{F}_q}(c \pmod{P_i}) = \text{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\delta_i c) = \delta_i \text{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(c). \tag{3.5}$$

https://doi.org/10.4153/S0008414X23000652 Published online by Cambridge University Press

We note that $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(c) \neq 0$ since $x^p - x - c$ is irreducible over $\mathbb{F}_q$. Therefore, (3.5) is nonzero; we use condition (i). Using the definition of the Rédei matrix R in Lemma 2.2, we get a $t \times t$ matrix $R = [r_{ij}]$ over $\mathbb{F}_p$ which is given in (3.4). Hence, the desired result follows.

For the case where $p = 2$, the 2-class group of Cl_K is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^t$ by the fact that λ_n gives the full 2^n-rank of Cl_K. By Lemma 2.6, the remaining result follows. ■

4 Computing the λ_3-rank of class groups of Artin–Schreier function fields

In this section, Algorithm 1 presents an explicit method for computing the λ_3-rank of the ideal class groups of Artin–Schreier extensions K over k. In Theorem 4.3, we provide a proof for Algorithm 1. In particular, we obtain an explicit method for determining the exact 2^3-rank of the ideal class groups of Artin–Schreier quadratic extensions over k (Corollary 4.4).

The following lemma plays a crucial role for the proof of Theorem 4.3.

Lemma 4.1 *Let $K = k(\alpha_{D_m})$ be the Artin–Schreier extension over k of extension degree p, where $D_m(T) = \sum_{i=1}^{m} \frac{Q_i}{P_i^{r_i}} + f(T)$ is defined as (2.1) and α_{D_m} is a root of $x^p - x = D_m$. For $1 \le i \le m$, let α_i be a root of $x^p - x = D_i := Q_i/P_i^{r_i}$ and let γ_i be a root of the following equation in $\overline{k}$:*

$$\mathbf{X}^p - \mathbf{X} = \mathcal{D}_i := \frac{{\alpha_i}^2 P_i^{r_i}}{Q_i}.$$

Then $k(\alpha_i, \gamma_i)/k(\alpha_i)$ is unramified, where all the infinite places of $k(\alpha_i)$ split completely in $k(\alpha_i, \gamma_i)$.

Proof We first show that $k(\alpha_i, \gamma_i)/k(\alpha_i)$ is an unramified extension. Let $\mathfrak{p}_i \in k(\alpha_i)$ be a place which lies above a finite place P of k. We note that it suffices to show the following by Lemma 2.4:

$$\nu_{\mathfrak{p}_i}(\mathcal{D}_i) = 2\nu_{\mathfrak{p}_i}(\alpha_i) + \nu_{\mathfrak{p}_i}(P_i^{r_i}) - \nu_{\mathfrak{p}_i}(Q_i) \ge 0. \tag{4.1}$$

We consider the following three possible cases: $P = P_i$ for $1 \le i \le m$, P divides $Q_i \in \mathbb{F}_q[T]$, and $(P, P_i) = (P, Q_i) = 1$. Using a valuation property, we can easily show the following, where n is a positive integer.

$$\text{If } \nu_{\mathfrak{p}_i}(\alpha_i^n - \alpha_i) < 0, \text{ then } \nu_{\mathfrak{p}_i}(\alpha_i^n - \alpha_i) = n\nu_{\mathfrak{p}_i}(\alpha_i) < 0. \tag{4.2}$$

$$\text{If } \nu_{\mathfrak{p}_i}(\alpha_i^n - \alpha_i) > 0, \text{ then } \nu_{\mathfrak{p}_i}(\alpha_i) \ge 0. \tag{4.3}$$

$$\text{If } \nu_{\mathfrak{p}_i}(\alpha_i^n - \alpha_i) = 0, \text{ then } \nu_{\mathfrak{p}_i}(\alpha_i^n - \alpha_i) = \nu_{\mathfrak{p}_i}(\alpha_i) = 0. \tag{4.4}$$

We denote *the ramification index of $\mathfrak{p}_i$ over P in $k(\alpha_i)/k$ by $e(\mathfrak{p}_i|P)$ and the residue class field degree of $\mathfrak{p}_i$ over P* by $f(\mathfrak{p}_i|P)$.

(i) Suppose that $P = P_i$. Then we have $e(\mathfrak{p}_i|P) = e(\mathfrak{p}_i|P_i) = p$ since P_i is the only totally ramified finite place for $k(\alpha_i)/k$. Therefore, we have $\nu_{\mathfrak{p}_i}(\alpha_i^p - \alpha_i) =$

https://doi.org/10.4153/S0008414X23000652 Published online by Cambridge University Press

$v_{\mathfrak{p}_i}(Q_i/P_i^{r_i}) = -pr_i < 0$; this implies that $v_{\mathfrak{p}_i}(\alpha_i) = -r_i$ by (4.2). Therefore, (4.1) holds true.

(ii) Suppose that P divides Q_i in $\mathbb{F}_q[T]$. Under the given assumption, we have $e(\mathfrak{p}_i|P) = 1$; this is because $(P, P_i) = 1$ as $(P_i, Q_i) = 1$ and P_i is the only totally ramified finite place for $k(\alpha_i)/k$. Consequently, we have

$$v_{\mathfrak{p}_i}(\alpha_i^p - \alpha_i) = v_{\mathfrak{p}_i}(Q_i/P_i^{r_i}) = v_P(Q_i/P_i^{r_i}) = v_P(Q_i) > 0;$$

thus, $v_{\mathfrak{p}_i}(\alpha_i) \geq 0$ by (4.3). Assuming that $v_{\mathfrak{p}_i}(\alpha_i) = 0$, we obtain

$$v_P(N_{k(\alpha_i)/k}(\alpha_i)) = f(\mathfrak{p}_i|P)v_{\mathfrak{p}_i}(\alpha_i) = 0. \tag{4.5}$$

However, since $v_{\mathfrak{p}_i}(N_{k(\alpha_i)/k}(\alpha_i)) = v_{\mathfrak{p}_i}(Q_i/P_i^{r_i}) > 0$ (4.5) cannot happen. Therefore, we have $v_{\mathfrak{p}_i}(\mathcal{D}_i) = 2v_P(Q_i) - v_P(Q_i) > 0$ and (4.1) follows; we use the fact that $v_{\mathfrak{p}_i}(\alpha_i) = v_P(Q_i) > 0$. As a result, $\mathfrak{p}_i$ is unramified in $k(\alpha_i, \gamma_i)$.

(iii) Suppose that $(P, P_i) = (P, Q_i) = 1$. In this case, we get $v_{\mathfrak{p}_i}(\alpha_i) = 0$ by (4.4) since $v_{\mathfrak{p}_i}(\alpha_i^p - \alpha_i) = 0$. Therefore, (4.1) follows immediately.

Now, it remains to show that all the infinite places of $k(\alpha_i)$ split completely in $k(\alpha_i, \gamma_i)$. Let $\mathfrak{p}_\infty$ (resp. $\mathfrak{P}_\infty$) be a place of $k(\alpha_i)$ (resp. $k(\alpha_i, \gamma_i)$) lying above the infinite place ∞ of k (resp. $\mathfrak{p}_\infty$). We first note that $v_{\mathfrak{p}_\infty}(\alpha_i^p - \alpha_i) = v_{\mathfrak{p}_\infty}(Q_i/P_i^{r_i}) > 0$; thus, $v_{\mathfrak{p}_\infty}(\alpha_i) \geq 0$ by (4.3). By a similar computation method as in (4.5), we obtain $v_{\mathfrak{p}_\infty}(\alpha_i) > 0$, and therefore $v_{\mathfrak{p}_\infty}(\alpha_i) = v_{\mathfrak{p}_\infty}(\alpha_i^p - \alpha_i) = \deg P_i^{r_i} - \deg Q_i$. Hence, we get

$$v_{\mathfrak{p}_\infty}(\mathcal{D}_i) = 2v_{\mathfrak{p}_\infty}(\alpha_i) + v_{\mathfrak{p}_\infty}(P_i^{r_i}) - v_{\mathfrak{p}_\infty}(Q_i) = 2(\deg P_i^{r_i} - \deg Q_i) - \deg P_i^{r_i} + \deg Q_i > 0;$$

from this fact and by Lemma 2.4, we can conclude that $\mathfrak{p}_\infty$ is unramified in $k(\alpha_i, \gamma_i)/k(\alpha_i)$.

Now, it is enough to show that $f(\mathfrak{P}_\infty|\mathfrak{p}_\infty)$ is 1. For the proof, we assume that $f(\mathfrak{P}_\infty|\mathfrak{p}_\infty) = p$. We first note that

$$N_{k(\alpha_i,\gamma_i)/k(\alpha_i)}(\gamma_i) = \gamma_i^p - \gamma_i = \alpha_i^2 P_i^{r_i}/Q_i. \tag{4.6}$$

On the other hand, we have

$$v_{\mathfrak{p}_\infty}(N_{k(\alpha_i,\gamma_i)/k(\alpha_i)}(\gamma_i)) = f(\mathfrak{P}_\infty|\mathfrak{p}_\infty)v_{\mathfrak{P}_\infty}(\gamma_i) = pv_{\mathfrak{P}_\infty}(\gamma_i). \tag{4.7}$$

Also, we can obtain

$$pv_{\mathfrak{P}_\infty}(\gamma_i) = v_{\mathfrak{p}_\infty}(\gamma_i^p - \gamma_i) = v_{\mathfrak{P}_\infty}(\gamma_i^p - \gamma_i), \tag{4.8}$$

by combining (4.6) with (4.7). Furthermore, since $v_{\mathfrak{p}_\infty}(\gamma_i^p - \gamma_i) = pv_{\mathfrak{P}_\infty}(\gamma_i) > 0$, we have

$$pv_{\mathfrak{P}_\infty}(\gamma_i) = \min\{pv_{\mathfrak{P}_\infty}(\gamma_i), v_{\mathfrak{P}_\infty}(\gamma_i)\} = v_{\mathfrak{P}_\infty}(\gamma_i), \tag{4.9}$$

which is a contradiction. Therefore, the infinite place of $k(\alpha_i)$ splits completely in $k(\alpha_i, \gamma_i)$. ∎

Lemma 4.2 *Let K be the Artin–Schreier extension over k of extension degree p. Let H_K be the Hilbert class field of K, and let $\mathcal{G}_K$ be the genus field of K. Let $\mathcal{H}$ be*

https://doi.org/10.4153/S0008414X23000652 Published online by Cambridge University Press

Algorithm 1 (Computation of λ_3 for the Artin–Schreier function field K)

Input:

- q : a power of a prime p
- $D_m(T) := \sum_{i=1}^{m} \frac{Q_i}{P_i^{r_i}} + f(T)$ defined by (2.1)
- $K = k(\alpha_{D_m})$ with α_{D_m} defined in (2.1)

Output: the λ_3-rank of the ideal class group of K

(1) Find λ_1 of K, and compute a Rédei matrix R over $\mathbb{F}_p$ using Lemma 2.2.
(2) Compute $\lambda_2 = \lambda_1 - \text{rank}(R)$.
(3) **If** $\lambda_2 = 0$, then **Stop**.
(4) **Else**
  (4.1) **If** $\lambda_2 < \lambda_1$, then let
  $\mathcal{I} := \{1 \le i \le m \mid \text{the } i\text{th row vector of } R \text{ is zero}\} = \{s_1, \dots, s_{\lambda_2}\}$ with $s_i < s_j$ for $1 \le i < j \le \lambda_2$.
  (4.2) **Else** let $\mathcal{I} := \{1, \dots, \lambda_2\} = \{s_1, \dots, s_{\lambda_2}\}$ with $i = s_i$ for $1 \le i \le \lambda_2$.
(5) **For** $1 \le i \le \lambda_2$,
  (5.1) set $\mathcal{P}_i := P_{s_i}$ and $\mathcal{F}_i := Q_{s_i}/P_{s_i}^{r_{s_i}}$.
  (5.2) let $\mathfrak{a}_i$ be a root of $x^p - x = \mathcal{F}_i$ in $\overline{k}$, and set $\mathcal{D}_i = \mathfrak{a}_i^2/\mathcal{F}_i$.
(6) **For** $1 \le i, j \le \lambda_2$,
  find a $\lambda_2 \times \lambda_2$-matrix $\mathcal{R} = [\mathfrak{r}_{ij}]$ over $\mathbb{F}_p$, where $\mathfrak{r}_{ij}$ is defined as $\mathfrak{r}_{ij} = \left\{\frac{\mathcal{D}_j}{\mathcal{P}_i}\right\}$.
(7) Compute $\lambda_3 = \lambda_2 - \text{rank}(\mathcal{R})$.

a fixed field of a subgroup of $\text{Gal}(H_K/\mathcal{G}_K)$ *which is isomorphic to* $Cl_K^{(\sigma-1)^2}$. *Then* $Cl_K(p)^{(\sigma-1)}/Cl_K(p)^{(\sigma-1)^2}$ *is isomorphic to* $\text{Gal}(\mathcal{H}/\mathcal{G}_K)$*; thus, we can define the following composite map:*

$$\Psi : Cl_K(p)^G \cap Cl_K(p)^{(\sigma-1)} \to Cl_K(p)^{(\sigma-1)}/Cl_K(p)^{(\sigma-1)^2} \xrightarrow{\simeq} \text{Gal}(\mathcal{H}/\mathcal{G}_K), \tag{4.10}$$

where the first map is induced by the inclusion map.

Then λ_3 *is equal to* $\lambda_2 - \text{rank}(\mathcal{R})$*, where* $\mathcal{R}$ *is a matrix representing* Ψ *over* $\mathbb{F}_p$ *and* λ_2 *is obtained by Lemma 2.2.*

Proof We note that $\text{Gal}(H_K/K) \simeq Cl_K$ and $\text{Gal}(\mathcal{G}_K/K) \simeq Cl_K(p)/Cl_K(p)^{(\sigma-1)} \simeq Cl_K/Cl_K^{(\sigma-1)}$ [19, pp. 328–329]; therefore, $\text{Gal}(H_K/\mathcal{G}_K) \simeq Cl_K^{(\sigma-1)}$. By the Galois correspondence, we have isomorphisms $\text{Gal}(\mathcal{H}/\mathcal{G}_K) \simeq Cl_K^{(\sigma-1)}/Cl_K^{(\sigma-1)^2}$ and $Cl_K^{(\sigma-1)}/Cl_K^{(\sigma-1)^2} \simeq Cl_K(p)^{(\sigma-1)}/Cl_K(p)^{(\sigma-1)^2}$; thus, we have the isomorphism $Cl_K(p)^{(\sigma-1)}/Cl_K(p)^{(\sigma-1)^2} \xrightarrow{\simeq} \text{Gal}(\mathcal{H}/\mathcal{G}_K)$.

Let Ψ be the map defined as in (4.10). Then we have

$$|\text{Ker}(\Psi)| = |Cl_K(p)^G \cap Cl_K(p)^{(\sigma-1)^2}|.$$

We claim that for any positive integer n,

$$|Cl_K(p)^G \cap Cl_K(p)^{(\sigma-1)^{n-1}}| = |Cl_K(p)^{(\sigma-1)^{n-1}}/Cl_K(p)^{(\sigma-1)^n}|. \tag{4.11}$$

https://doi.org/10.4153/S0008414X23000652 Published online by Cambridge University Press

We consider a short exact sequence

$$0 \to Cl_K(p)^G \cap Cl_K(p)^{(\sigma-1)^{n-1}} \xrightarrow{\imath} Cl_K(p)^{(\sigma-1)^{n-1}} \xrightarrow{\sigma-1} Cl_K(p)^{(\sigma-1)^n} \to 0,$$

where $\imath$ denotes an inclusion map. Then $Cl_K(p)^{(\sigma-1)^n}$ is isomorphic to

$$Cl_K(p)^{(\sigma-1)^{n-1}}/\mathrm{Im}(\imath) = Cl_K(p)^{(\sigma-1)^{n-1}}/Cl_K(p)^G \cap Cl_K(p)^{(\sigma-1)^{n-1}}.$$

Therefore, we have the following:

$$|Cl_K(p)^{(\sigma-1)^n}| = \frac{|Cl_K(p)^{(\sigma-1)^{n-1}}|}{|Cl_K(p)^G \cap Cl_K(p)^{(\sigma-1)^{n-1}}|}.$$

We can rewrite this as

$$|Cl_K(p)^G \cap Cl_K(p)^{(\sigma-1)^{n-1}}| = \frac{|Cl_K(p)^{(\sigma-1)^{n-1}}|}{|Cl_K(p)^{(\sigma-1)^n}|} = |Cl_K(p)^{(\sigma-1)^{n-1}}/Cl_K(p)^{(\sigma-1)^n}|;$$

hence, (4.11) follows.

Therefore, we compute as follows:

$$\begin{aligned}
\lambda_3 &= \dim_{\mathbb{F}_p}(Cl_K(p)^{(\sigma-1)^2}/Cl_K(p)^{(\sigma-1)^3}) = \dim_{\mathbb{F}_p}(Cl_K(p)^G/Cl_K(p)^{(\sigma-1)^2}) \\
&= \dim_{\mathbb{F}_p}(\mathrm{Ker}(\Psi)) = \dim_{\mathbb{F}_p}(Cl_K(p)^G \cap Cl_K(p)^{(\sigma-1)}) - \dim_{\mathbb{F}_p}(\mathrm{Im}(\Psi)) \\
&= \dim_{\mathbb{F}_p}(Cl_K(p)^{(\sigma-1)}/Cl_K(p)^{(\sigma-1)^2}) - \dim_{\mathbb{F}_p}(\mathrm{Im}(\Psi)) = \lambda_2 - \dim_{\mathbb{F}_p}(\mathrm{Im}(\Psi)) \\
&= \lambda_2 - \mathrm{rank}(\mathcal{R}),
\end{aligned}$$

where $\mathcal{R}$ is a matrix representing Ψ over $\mathbb{F}_p$ and λ_2 is obtained by Lemma 2.2. We note that the second equality and the fifth one hold by (4.11) with $n = 3$ and 2, respectively. ■

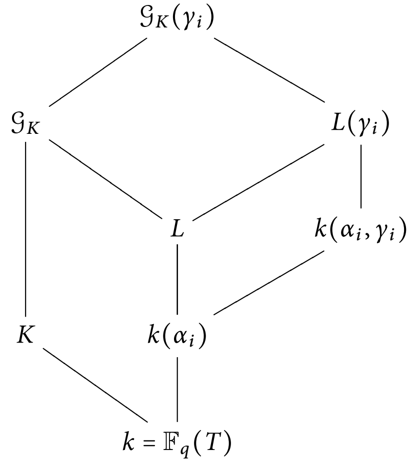
Theorem 4.3 *Let K be the Artin–Schreier extension over the rational function field k of extension degree p. Then the λ_3-rank of the ideal class group of K can be computed by Algorithm 1.*

Proof By Lemma 4.2, we have $\lambda_3 = \lambda_2 - \mathrm{rank}(\mathcal{R})$, where $\mathcal{R}$ is a matrix representing Ψ which is defined as in (4.10). Therefore, it is sufficient to compute the matrix $\mathcal{R}$ in an explicit way for computation of λ_3. We describe how to compute the matrix $\mathcal{R}$ as follows.

Let $\mathcal{I} := \{1 \le i \le m \mid \text{the } i\text{th row vector of } R \text{ is zero}\} = \{s_1, \ldots, s_{\lambda_2}\}$, where $s_i < s_j$ for $1 \le i < j \le \lambda_2$. For simplicity, we set $\mathcal{P}_i := P_{s_i}$ and $\mathcal{F}_i = Q_{s_i}/P_{s_i}^{r_{s_i}}$ for $1 \le i \le \lambda_2$. Let $\mathcal{D}_i := \mathfrak{a}_i{}^2/\mathcal{F}_i$, and let γ_i be a root of $\mathbf{X}^p - \mathbf{X} = \mathcal{D}_i$ in $\overline{k}$, where $\overline{k}$ is the algebraic closure of k and $\mathfrak{a}_i$ is the root of $x^p - x = \mathcal{F}_i$ in $\overline{k}$.

Let $L := k(\alpha_1, \ldots, \alpha_m)$ be a subfield of the genus field $\mathcal{G}_K$ defined as the following, where $\mathcal{G}_K$ is given in Lemma 2.3.

https://doi.org/10.4153/S0008414X23000652 Published online by Cambridge University Press



We now show that $\mathcal{G}_K(\gamma_i)$ is a subfield of H_K for $1 \le i \le \lambda_2$. We point out that $\mathcal{G}_K(\gamma_i)/\mathcal{G}_K$ is an abelian extension by the fact that it is the Artin–Schreier function field. It suffices to show that $\mathcal{G}_K(\gamma_i)/\mathcal{G}_K$ is an unramified extension and all the infinite places of $\mathcal{G}_K$ split completely in $\mathcal{G}_K(\gamma_i)$. By Lemma 4.1, $k(\alpha_i, \gamma_i)/k(\alpha_i)$ is an unramified extension and all the infinite places of $k(\alpha_i)$ split completely in $k(\alpha_i, \gamma_i)$. Thus, $L(\gamma_i)/L$ is an unramified extension; hence, $\mathcal{G}_K(\gamma_i)/\mathcal{G}_K$ is an unramified extension.

Now, we show that all the infinite places of $\mathcal{G}_K$ split completely in $\mathcal{G}_K(\gamma_i)$. Every infinite place of $k(\alpha_i)$ splits completely in $k(\alpha_i, \gamma_i)$ as shown above and all the infinite places of L split completely in $L(\gamma_i)$. Also, all the infinite places split completely in $L/k(\alpha_i)$ by Lemma 2.1. Consequently, all the infinite places of L split completely in the compositum $L(\gamma_i)$ of L and $k(\alpha_i, \gamma_i)$.

Let $\mathcal{P}_\infty$ be a place of L which lies above the infinite place ∞ of k and $\mathcal{P}'$ a place of $\mathcal{G}_K$ which lies above $\mathcal{P}_\infty$. We consider the following two possible cases: $\mathcal{P}_\infty$ splits completely in $\mathcal{G}_K$ or $\mathcal{P}_\infty$ is totally ramified or inert in $\mathcal{G}_K$. We note that the result follows immediately in the former case; thus, it is sufficient to consider the latter case where there is exactly one place lying above $\mathcal{P}_\infty$ in $\mathcal{G}_K$, the number of places in $\mathcal{G}_K(\gamma_i)$ which lie above $\mathcal{P}'$ is exactly p; this is because the infinite places split completely in $L(\gamma_i)/L$. Therefore, $\mathcal{P}'$ splits completely in $\mathcal{G}_K(\gamma_i)$, and the result holds.

We have $\mathcal{H} = \mathcal{G}_K(\gamma_1, \ldots, \gamma_{\lambda_2})$ since $\mathcal{G}_K(\gamma_i) \subseteq H_K$ and $[\mathcal{H} : \mathcal{G}_K] = p^{\lambda_2}$. We get

$$\left(\frac{\mathcal{H}/\mathcal{G}_K}{\mathfrak{p}_i}\right)(\gamma_j) = \gamma_j + \left\{\frac{\mathcal{D}_j}{\mathcal{P}_i}\right\},$$

where $\mathfrak{p}_i$ is a place of $\mathcal{G}_K$ lying above $\mathcal{P}_i$ for $1 \le i \le \lambda_2$ by the action of the Artin map in the Artin–Schreier function field. Therefore, we determine $\mathcal{R} = [\mathfrak{r}_{ij}] = \left\{\frac{\mathcal{D}_j}{\mathcal{P}_i}\right\}$.

This process is implemented in Algorithm 1. Steps (1) and (2) of Algorithm 1 give the process of computing λ_1, λ_2, and the Rédei matrix R. Step (3) explains the case where $\lambda_2 = 0$ and then the algorithm stops. If $0 < \lambda_2 < \lambda_1$, then we go to Step (4.1), and if $\lambda_2 = \lambda_1$, then we proceed with Step (4.2). Steps (5.1) and (5.2) explain the process of finding $\mathcal{D}_i$ for $1 \le i \le \lambda_2$. In Step (6), we determine a matrix $\mathcal{R}$ over $\mathbb{F}_p$, and finally we obtain $\lambda_3 = \lambda_2 - \text{rank}(\mathcal{R})$ in Step (7). ∎

Corollary 4.4 *Let K be the Artin–Schreier quadratic extension over k, and let the λ_3-rank of Cl_K be computed by Algorithm 1. Then the 2^3-rank of Cl_K is exactly λ_3: that is, $Cl_K(2)$ has a subgroup isomorphic to $(\mathbb{Z}/2^3\mathbb{Z})^{\lambda_3}$.*

Proof This follows immediately from the fact that λ_n is exactly equal to the full 2^n-rank of Cl_K and Theorem 4.3. ∎

Remark 4.5 For readers, focusing on the case: $p = 2$, we first briefly explain the analogy between Rédei symbols (the 4-rank of the class groups) and the 8-rank of the class groups in the quadratic field case (for more details, see [9]). Then we describe the analogy between Artin–Schreier quadratic extensions over k and quadratic extensions over $\mathbb{Q}$ for computation of λ_3.

Let F be a quadratic extension over $\mathbb{Q}$, and let Cl_F be the ideal class group of F. Let r_4 (resp. r_8) be the 2^2-rank (resp. 2^3-rank) of Cl_F. Let H be the Hilbert class field of F, and let H_n be the unramified abelian subextension of H such that $\mathrm{Gal}(H_n/F) \simeq Cl_F/Cl_F^n$ for $n = 2, 4$.

Basically, a strategy for computing the 2^2-rank (resp. 2^3-rank) is explicitly finding a subextension H_2 (resp. H_4) of the Hilbert class field of F whose Galois group is isomorphic to $\mathrm{Gal}(Cl_F/Cl_F^2)$ (resp. $\mathrm{Gal}(Cl_F^2/Cl_F^4)$).

Define two maps as follows:

$$R_4 : \mathbb{F}_2^t \to Cl_F[2] \xrightarrow{\varphi} Cl_F/Cl_F^2 \xrightarrow{\simeq} \mathrm{Gal}(H_2/F) \to \mathrm{Gal}(H_2/\mathbb{Q}) = \prod_{i=1}^{t} \mathrm{Gal}(\mathbb{Q}(\sqrt{d_i})/\mathbb{Q}),$$

$$R_8 : \mathrm{Ker}\, R_4 \to Cl_F[2] \cap Cl_F^2 \xrightarrow{\psi} Cl_F^2/Cl_F^4 \xrightarrow{\simeq} \mathrm{Gal}(H_4/H_2) = \prod_{i=1}^{r_4} \mathrm{Gal}(H_2(\sqrt{\alpha_i})/H_2) \to \mathbb{F}_2^{r_4},$$

where t is the number of finite primes of $\mathbb{Q}$ which are ramified in F, $Cl_F[2]$ is the 2-torsion part of Cl_F, and the maps φ and ψ are induced by the inclusion maps. For computation of r_4 and r_8, we find appropriate d_i $(1 \le i \le t)$ and α_i $(1 \le i \le r_4)$. Then we have

$$r_4 = t - \dim_{\mathbb{F}_2} R_4 \quad \text{and} \quad r_8 = r_4 - \dim_{\mathbb{F}_2} R_8.$$

To show the analogy between Artin–Schreier quadratic extensions over k and quadratic extensions over $\mathbb{Q}$ for computation of λ_3 (2^3-rank), let K be the Artin–Schreier quadratic extension over k. Then the map R_8 corresponds to the map Ψ defined in (4.10):

$$\Psi : Cl_K(2)^G \cap Cl_K^2 \to Cl_K^2/Cl_K^4 \xrightarrow{\simeq} \mathrm{Gal}(\mathcal{H}/\mathcal{G}_K).$$

Then we have $\lambda_3 = \lambda_2 - \mathrm{rank}\,\mathcal{R}$, where $\mathcal{R}$ is a matrix over $\mathbb{F}_2$ representing the map Ψ. We recall that λ_3 is the 2^3-rank of Cl_K.

5 An infinite family of Artin–Schreier function fields with higher λ_n-rank

In this section, we find an infinite family of Artin–Schreier function fields which have *prescribed* λ_n-rank of the ideal class group for $1 \le n \le 3$. In Theorem 5.1, for any positive integer $t \ge 2$, we obtain an infinite family of Artin–Schreier extensions over k

https://doi.org/10.4153/S0008414X23000652 Published online by Cambridge University Press

whose λ_1-rank is t, λ_2-rank is $t-1$, and λ_3-rank is $t-2$. Then Corollary 5.3 shows the case where $p=2$, for a given positive integer $t \geq 2$, we obtain an infinite family of the Artin–Schreier quadratic extensions over k whose 2-class group rank (resp. 2^2-class group rank and 2^3-class group rank) is *exactly* t (resp. $t-1$ and $t-2$). Furthermore, we also obtain a similar result on the 2^n-ranks of the divisor class groups of the Artin–Schreier quadratic extensions over k in Corollary 5.4.

Throughout this section, we define D_m as follows.

Notation 1 *Let $D_m := \sum_{i=1}^{m} D_i + f(T)$ be defined in (2.1) with $D_i = Q_i/P_i^{r_i}$, where m, P_i, Q_i, and $f(T)$ satisfy one of the followings:*

(i) $m = \begin{cases} t, & \text{if } \deg f(T) \geq 1 \\ & \text{or } f(T) = c \in \mathbb{F}_q^\times \text{ such that } x^p - x = c \text{ is irreducible over } \mathbb{F}_q, \\ t+1, & \text{if } f(T) = 0. \end{cases}$

(ii) *$Q_j \equiv P_j^{r_j}(b_i(T)^q - b_i(T)) \pmod{P_i}$ for any $1 \leq i \neq j \leq m$ except $(i,j) = (1,2)$, where $b_i(T) \in \mathbb{F}_q[T]$.*

(iii) *If $\deg f(T) \geq 1$, then $f(T) \equiv P_j^{r_j}(b_i(T)^q - b_i(T)) \pmod{P_i}$, where $b_i(T) \in \mathbb{F}_q[T]$ for any $1 \leq i \leq m$.*

(iv) *If $f(T) \in \mathbb{F}_q^\times$, then $q \mid \deg P_i$ for any i with $1 \leq i \leq m$.*

(v) *$Q_j^{-1} \equiv P_j^{r_j}(b_i(T)^q - b_i(T)) \pmod{P_i}$, where $b_i(T) \in \mathbb{F}_q[T]$ and Q_j^{-1} denotes the inverse of Q_j modulo P_i for any $1 \leq i \neq j \leq m$ except $(i,j) \neq (1,2)$.*

Theorem 5.1 *For a given positive integer $t \geq 2$, there is an infinite family of Artin–Schreier extensions over k whose λ_1-rank is t, λ_2-rank is $t-1$, and λ_3-rank is $t-2$.*

Let $K = k(\alpha_{D_m})$ be the Artin–Schreier function field over k of extension degree p, where D_m is defined in Notation 1 and α_{D_m} is a root of $x^p - x = D_m$. Then the ideal class group Cl_K of K has $\lambda_1 = t$, $\lambda_2 = t-1$, and $\lambda_3 = t-2$.

Remark 5.2 Let $\mathbb{F}_q$ be a finite field of order q, t be a given integer, and $f(T) \in \mathbb{F}_q$. By condition (i), $m = t+1$. By condition (ii), we can choose monic irreducible polynomials $P_i \in \mathbb{F}_q[T]$ whose degrees are divisible by p. We note that conditions (iii) and (iv) can be interpreted as

$$\left\{\frac{D_j}{P_i}\right\} = \left\{\frac{Q_j^{-1}}{P_i}\right\} = 0; \tag{5.1}$$

by the surjectivity of the trace map, there always exist D_j and Q_j^{-1} which satisfy (5.1). Since our choice of P_i's are infinite, we have an infinite family of Artin–Schreier extensions which satisfy the conditions in Theorem 5.1.

Proof of Theorem 5.1 Recall that $\lambda_2 = \lambda_1 - \operatorname{rank}(R)$ and $\lambda_3 = \lambda_2 - \operatorname{rank}(\mathcal{R})$, where R (resp. $\mathcal{R}$) is a matrix over $\mathbb{F}_p$ defined in Lemma 2.2 (resp. Algorithm 1). We need to show that

$$\lambda_1 = t, \qquad \lambda_2 = t-1, \qquad \lambda_3 = t-2; \tag{5.2}$$

this is equivalent to $\operatorname{rank}(R) = \operatorname{rank}(\mathcal{R}) = 1$.

We divide into the following three cases: $\deg f(T) \geq 1$, $\deg f(T) = 0$, and $f(T) = c$, where $x^p - x - c$ is irreducible over $\mathbb{F}_q$.

https://doi.org/10.4153/S0008414X23000652 Published online by Cambridge University Press

Case I. $\deg f(T) \geq 1$: that is, the infinite place of k is totally ramified in K.

Since $\deg f(T) \geq 1$, we have $m = t$ by condition (i); this implies that $\lambda_1 = m = t$ by Lemma 2.2. For computing λ_2, we compute every entry of the Rédei matrix R: that is, the Hasse norm $\{D_j/P_i\}$ and $\{f(T)/P_i\}$ for $1 \leq i \neq j \leq m$. Using Lemma 3.1 and condition (ii), we can easily obtain that $\left\{\frac{D_2}{P_1}\right\} \neq 0$ and $\left\{\frac{D_j}{P_i}\right\} = 0$ for any $1 \leq i \neq j \leq m$ except $(i, j) \neq (1, 2)$. Furthermore, we get $\left\{\frac{f}{P_i}\right\} = 0$ for any $1 \leq i \leq m$ by condition (iii). Therefore, the Rédei matrix R can be written as $R = \begin{bmatrix} p-1 & 1 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{bmatrix}$; thus, $\lambda_2 = \lambda_1 - \operatorname{rank}(R) = t - 1$. Lastly, we compute λ_3 of K using Algorithm 1 and Theorem 4.3. Using the definition of a matrix $\mathcal{R}$ which is given in Algorithm 1, it suffices to compute $\left\{\frac{1/Q_j}{P_i}\right\}$ for $1 \leq i \neq j \leq m$. By the same reasoning as in the computation of R, we get $\lambda_3 = \lambda_2 - \operatorname{rank}(\mathcal{R}) = t - 2$. Therefore, (5.2) follows.

Case II. $\deg f(T) = 0$: that is, the infinite place of k splits completely in K, which is a real extension.

We can easily obtain $\lambda_1 = t$ by using Lemma 2.2 and the condition $m = t + 1$. For computing λ_2, we compute every entry of the Rédei matrix R: that is, the value of Hasse norm $\{D_j/P_i\}$ for $1 \leq i \neq j \leq m$. By the definition of Hasse norm which is defined in Definition 2.1, we get $\{D_2/P_1\} \neq 0$ and $\{D_j/P_i\} = 0$, where $1 \leq i \neq j \leq m$ except $(i, j) = (1, 2)$. As in Case 1, the rank of Rédei matrix is one: that is, $\lambda_2 = \lambda_1 - \operatorname{rank}(R) = t - 1$. Lastly, we compute λ_3 of K; by the same computation method as in Case I, we have $\lambda_3 = \lambda_2 - \operatorname{rank}(\mathcal{R}) = t - 2$. Therefore, (5.2) follows.

Case III. $f(T) = c \in \mathbb{F}_q^{\times}$, where $x^p - x - c$ is irreducible over $\mathbb{F}_q$: that is, the infinite place of k is inert in K.

Under this assumption, K is an imaginary extension; so, $m = t$. We claim that (5.2) holds for this case. We can simply get $\lambda_1 = t$ by Lemma 2.2 and we also obtain $\{D_j/P_i\} = 0$ for every $1 \leq i \neq j \leq t = m$ except $(i, j) = (1, 2)$ by using the same reasoning as in Case I. Now, we compute the value of $\{c/P_i\}$ for $1 \leq i \leq t = m$, where $c \in \mathbb{F}_q^{\times}$. We have

$$\left\{\frac{c}{P_i}\right\} = \operatorname{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\operatorname{Tr}_{\mathbb{F}_\mathfrak{d}/\mathbb{F}_q} c) = \operatorname{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(c \deg P_i) = \deg P_i(\operatorname{Tr}_{\mathbb{F}_q/\mathbb{F}_p} c);$$

the second equation holds since c is a nonzero element of $\mathbb{F}_q$ and the last equation holds by the property of a trace map over a finite field. We get $\deg P_i(\operatorname{Tr}_{\mathbb{F}_q/\mathbb{F}_p} c) = 0$ in $\mathbb{F}_p$ by Lemma 3.1 by the assumption that $q \mid \deg P_i$ for every $1 \leq i \leq m$; therefore, (3.5) is zero in $\mathbb{F}_p$. Hence, $\lambda_2 = t - 1$. By the same reasoning as in Case I, $\lambda_3 = t - 2$ and we have (5.2). ■

Corollary 5.3 *Let $K = k(\alpha_{D_m})$ be the Artin–Schreier quadratic function field over k of extension degree 2, where D_m is defined in Notation 1 and α_{D_m} is a root of $x^2 - x = D_m$.*

For any positive integer $t \geq 2$, there is an infinite family of Artin–Schreier quadratic extensions over k whose 2-class group rank is exactly t, 2^2-class group rank is $t - 1$, and 2^3-class group rank is $t - 2$.

In particular, $Cl_K(2)$ contains a subgroup isomorphic to $(\mathbb{Z}/2^n\mathbb{Z})^{t-n+1}$ for $1 \leq n \leq 3$.

https://doi.org/10.4153/S0008414X23000652 Published online by Cambridge University Press

Proof We note that λ_n is exactly equal to the full 2^n-rank ($1 \le n \le 3$) of the ideal class group Cl_K of K; therefore, the result follows immediately from Theorem 5.1. ■

Corollary 5.4 *For a given positive integer t, let $K = k(\alpha_{D_m})$ be the Artin–Schreier quadratic function field over k, where $D_m = \sum_{i=1}^{m} Q_i/P_i^{r_i} + f(T)$ such that $P_i, Q_i, f(T)$, and m satisfy the conditions (i)–(v) in Notation 1. Let J_K be the divisor class group of K. Then we have the following infinite family of Artin–Schreier quadratic extensions.*

(i) *For $t \ge 2$, if $\deg f(T) \ge 1$ (equivalently, ∞ is totally ramified in K), then the 2^n-class group rank of J_K is exactly equal to $t + 1 - n$ for $1 \le n \le 3$.*
(ii) *For $t \ge 2$, if $f(T) = 0$ (equivalently, ∞ splits completely in K), then the 2^n-class group rank of J_K is exactly either $t + 1 - n$ or $t + 2 - n$ for $1 \le n \le 3$.*
(iii) *For $t \ge 3$, if $f(T) \in \mathbb{F}_q^\times$ (equivalently, ∞ is inert in K), then the 2^n-class group rank of J_K is exactly either $t + 1 - n$ or $t - n$ for $1 \le n \le 3$.*

Proof Since D_m satisfies the conditions (i)–(v) in Notation 1, the ideal class group Cl_K of K has λ_1-rank t, λ_2-rank $t - 1$, and λ_3-rank $t - 2$.

We first assume that $\deg f(T) \ge 1$: that is, the infinite place ∞ of k is totally ramified in K. Then the ideal class group Cl_K of K is isomorphic to the divisor class group J_K of K by Lemma 2.6. Thus, by Lemma 5.3, the 2^n-rank of the divisor class group J_K of K is $t + 1 - n$ for n up to 3; thus, (i) follows.

Next, suppose that $f(T) = 0$. This is the case where the infinite place ∞ of k splits completely in K. Then, by Lemma 2.6, we note that J_K/R is isomorphic to Cl_K, where R denotes the group $\mathcal{D}_K^0(S)/\mathcal{P}_K(S)$. By the fact the group R is a cyclic group, the 2^n-rank of the divisor class group J_K is either $t + 1 - n$ or $t + 2 - n$ for n up to 3.

Finally, we assume that $f(T) \in \mathbb{F}_q^\times$: the case where ∞ is inert in K. Then, by the exact sequence given in Lemma 2.6(ii), we get $|Cl_K| = 2|J_K|$. Since $Cl_K(2)$ contains a subgroup isomorphic to $(\mathbb{Z}/2^n\mathbb{Z})^{t-n+1}$ for $1 \le n \le 3$, $J_K(2)$ contains a subgroup isomorphic to $(\mathbb{Z}/2^n\mathbb{Z})^{t-n+1}$ or $(\mathbb{Z}/2^n\mathbb{Z})^{t-n}$ for $1 \le n \le 3$; therefore, (iii) holds. ■

Remark 5.5 We briefly mention that the λ_2-rank is connected to the embedding problem. For instance, in the quadratic number field $F = \mathbb{Q}(\sqrt{d})$, the solvability of the conics $X^2 = aY^2 + \frac{d}{a}Z^2$ yields unramified cyclic quartic extensions of F. The solvability of this conic is related to the λ_2-rank of Cl_F, which is computed by the Rédei matrix in terms of Legendre symbols. Then the embedding problem for F is not solvable. On the other hand, in our context, the embedding problem for Artin–Schreier extensions K over k is solvable and every finite place of k is wildly ramified in K.

6 Implementation results

In this section, as implementation results, we explicitly present concrete infinite families of Artin–Schreier extensions over k whose ideal class groups have guaranteed prescribed λ_n-rank of the ideal class group for $1 \le n \le 3$. In Table 1, for a given positive integer t, we obtain explicit families of Artin–Schreier extensions K over k whose λ_1-rank of the ideal class group Cl_K is t and λ_n-rank is zero for $n \ge 2$, depending on the ramification behavior of the infinite place ∞ of k (Theorems 3.2–3.4). Furthermore, in Table 2, for a given integer $t \ge 2$, we get explicit families of Artin–Schreier extensions

https://doi.org/10.4153/S0008414X23000652 Published online by Cambridge University Press

<table>
<tr><th>t</th><th>p</th><th>q</th><th>$D = \sum Q_i/(P_i^{r_i}) + f$</th><th>Ideal class group</th><th>Divisor class group</th><th>∞</th></tr>
<tr><td>1</td><td>2</td><td>2</td><td>$\frac{1}{T} + T + \zeta$</td><td colspan="2">$\mathbb{Z}_2$</td><td></td></tr>
<tr><td></td><td></td><td></td><td>$\frac{1}{T^3} + T + \zeta$</td><td colspan="2">$\mathbb{Z}_2 \times \mathbb{Z}_{13}$</td><td></td></tr>
<tr><td></td><td></td><td></td><td>$\frac{1}{T^3+\zeta T^2+1} + T^3 + \zeta T^2 + \zeta^2$</td><td colspan="2">$\mathbb{Z}_2 \times (\mathbb{Z}_3)^2 \times \mathbb{Z}_5$</td><td></td></tr>
<tr><td></td><td>3</td><td>3^2</td><td>$\frac{1}{T^2} + T + \zeta$</td><td colspan="2">$(\mathbb{Z}_2)^4 \times \mathbb{Z}_3 \times \mathbb{Z}_{13}$</td><td></td></tr>
<tr><td></td><td></td><td></td><td>$\frac{1}{(T+\zeta)^2} + T^2 + T + 1$</td><td colspan="2">$\mathbb{Z}_3 \times \mathbb{Z}_{13} \times \mathbb{Z}_{103}$</td><td></td></tr>
<tr><td></td><td></td><td></td><td>$\frac{T+\zeta^5}{T^2+\zeta^3 T+1} + T^4 + \zeta^3 T^3 + T^2 + \zeta$</td><td colspan="2">$(\mathbb{Z}_2)^2 \times \mathbb{Z}_3 \times \mathbb{Z}_7 \times \mathbb{Z}_{79} \times \mathbb{Z}_{139}$</td><td>Totally</td></tr>
<tr><td>2</td><td>2</td><td>2^2</td><td>$\frac{T+1}{T^3} + \frac{T}{T^3+T+1} + T^3 + T + \zeta$</td><td colspan="2">$(\mathbb{Z}_2)^2 \times \mathbb{Z}_5 \times \mathbb{Z}_{101}$</td><td>ramified</td></tr>
<tr><td></td><td></td><td></td><td>$\frac{T+1}{T^3} + \frac{T}{T^3+T+1} + T^5 + T^3 + T^2 + \zeta$</td><td colspan="2">$(\mathbb{Z}_2)^2 \times (\mathbb{Z}_3)^2 \times \mathbb{Z}_5 \times \mathbb{Z}_{5^2}$</td><td></td></tr>
<tr><td></td><td>3</td><td>3^2</td><td>$\frac{\zeta T+\zeta^3}{T^2} + \frac{\zeta T}{T^2+\zeta T+\zeta^3} + T^2 + \zeta T + \zeta^5$</td><td colspan="2">$(\mathbb{Z}_2)^2 \times (\mathbb{Z}_3)^2 \times \mathbb{Z}_{19} \times \mathbb{Z}_{9643}$</td><td></td></tr>
<tr><td></td><td></td><td></td><td>$\frac{T+\zeta^6}{T^2} + \frac{T}{T^2+T+\zeta^7} + T^2 + T + \zeta$</td><td colspan="2">$(\mathbb{Z}_3)^3 \times \mathbb{Z}_{223} \times \mathbb{Z}_{10789}$</td><td></td></tr>
<tr><td>1</td><td>2</td><td>2^2</td><td>$\frac{T+1}{T^3} + \frac{\zeta(T+1)}{T^3+T+1}$</td><td>$\mathbb{Z}_2 \times \mathbb{Z}_3$</td><td>$\mathbb{Z}_2 \times (\mathbb{Z}_3)^2 \times \mathbb{Z}_5 \times \mathbb{Z}_7$</td><td></td></tr>
<tr><td></td><td></td><td></td><td>$\frac{\zeta T^2+T}{(T+1)^3} + \frac{1}{T^3+\zeta^2 T^2+1}$</td><td>$\mathbb{Z}_2$</td><td>$\mathbb{Z}_2 \times \mathbb{Z}_5 \times \mathbb{Z}_{83}$</td><td></td></tr>
<tr><td></td><td></td><td></td><td>$\frac{\zeta T^2+T}{(T+1)^3} + \frac{\zeta}{T^3+\zeta^2 T^2+1}$</td><td>$\mathbb{Z}_2$</td><td>$\mathbb{Z}_2 \times \mathbb{Z}_{71}$</td><td></td></tr>
<tr><td></td><td>3</td><td>3^2</td><td>$\frac{1}{T^2} + \frac{\zeta T+\zeta^6}{T^2+2T+\zeta}$</td><td>$\mathbb{Z}_3$</td><td>$\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_7 \times \mathbb{Z}_{1069}$</td><td></td></tr>
<tr><td></td><td></td><td></td><td>$\frac{T^3+\zeta^5 T}{(T+\zeta)^4} + \frac{\zeta^5}{T+\zeta^2}$</td><td>$\mathbb{Z}_3$</td><td>$\mathbb{Z}_3 \times (\mathbb{Z}_{23})^2 \times \mathbb{Z}_{37}$</td><td>Splits</td></tr>
<tr><td></td><td></td><td></td><td>$\frac{T+\zeta^5}{T^2+\zeta^3 T+1} + \frac{\zeta^3 T+\zeta^3}{(T+\zeta^3)^2}$</td><td>$(\mathbb{Z}_{2^2})^2 \times \mathbb{Z}_3 \times \mathbb{Z}_7$</td><td>$(\mathbb{Z}_{2^2})^2 \times (\mathbb{Z}_3)^2 \times \mathbb{Z}_{37}$</td><td>completely</td></tr>
</table>

Table 1: Infinite families of Artin–Schreier extensions $K = k(\alpha_D)$ over k whose λ_1-rank of the ideal class groups is t and λ_n-rank is zero for $n \geq 2$, where $\alpha_D^p - \alpha_D = D$.

t	p	q	$D = \sum Q_i/(P_i^{r_i}) + f$	Ideal class group	Divisor class group	∞
2	2	2^2	$\frac{T+1}{T^3} + \frac{T}{T^3+T+1} + \frac{T^2+\zeta T+\zeta^2}{(T+\zeta)^5}$	$(\mathbb{Z}_2)^2$	$(\mathbb{Z}_2)^2 \times (\mathbb{Z}_{3^2}) \times \mathbb{Z}_{17} \times \mathbb{Z}_{37}$	
			$\frac{T+1}{T^3} + \frac{\zeta}{T^3+T+1} + \frac{T^2+\zeta T+\zeta^2}{(T+\zeta)^5}$	$(\mathbb{Z}_2)^2$	$\mathbb{Z}_2 \times \mathbb{Z}_{2^2} \times \mathbb{Z}_7 \times \mathbb{Z}_{13} \times \mathbb{Z}_{17}$	
	3	3^2	$\frac{\zeta T+\zeta^3}{T^2} + \frac{\zeta T}{T^2+\zeta T+\zeta^3} + \frac{\zeta^5 T+\zeta^2}{(T+\zeta)^2}$	$(\mathbb{Z}_3)^2$	$(\mathbb{Z}_3)^2 \times \mathbb{Z}_{3434467}$	
			$\frac{\zeta T+\zeta^3}{T^2} + \frac{\zeta T}{T^2+\zeta T+\zeta^3} + \frac{\zeta^2}{(T+\zeta)^2}$	$(\mathbb{Z}_3)^2$	$(\mathbb{Z}_3)^2 \times \mathbb{Z}_{31} \times \mathbb{Z}_{139} \times \mathbb{Z}_{1279}$	
1	2	2^2	$\frac{1}{T} + \zeta$	$\mathbb{Z}_2$	Identity	
			$\frac{T^2+\zeta T+1}{T^3} + \zeta^2$	$\mathbb{Z}_2 \times \mathbb{Z}_5$	$\mathbb{Z}_5$	
			$\frac{1}{T^3+\zeta T^2+1} + \zeta$	$\mathbb{Z}_2 \times \mathbb{Z}_{17}$	$\mathbb{Z}_{17}$	
	3	3^2	$\frac{1}{T^2} + 1$	$\mathbb{Z}_3 \times \mathbb{Z}_7$	$\mathbb{Z}_7$	
			$\frac{T^3+\zeta^5 T}{(T+\zeta)^4} + 2$	$(\mathbb{Z}_{2^2})^2 \times \mathbb{Z}_3 \times (\mathbb{Z}_5)^2$	$(\mathbb{Z}_{2^2})^2 \times (\mathbb{Z}_5)^2$	
			$\frac{T+\zeta^5}{T^2+\zeta^3 T+1} + \zeta^7$	$\mathbb{Z}_3 \times \mathbb{Z}_{97}$	$\mathbb{Z}_{97}$	Inert
2	2	2^2	$\frac{T+1}{T^3} + \frac{T}{T^3+T+1} + \zeta$	$(\mathbb{Z}_2)^2 \times \mathbb{Z}_{113}$	$\mathbb{Z}_2 \times \mathbb{Z}_{113}$	
			$\frac{T+1}{T^5} + \frac{T}{T^3+T+1} + \zeta^2$	$(\mathbb{Z}_2)^2 \times \mathbb{Z}_{227}$	$\mathbb{Z}_2 \times \mathbb{Z}_{277}$	
	3	3^2	$\frac{\zeta T+\zeta^3}{T^2} + \frac{\zeta T}{T^2+\zeta T+\zeta^3} + \zeta^5$	$(\mathbb{Z}_3)^3 \times (\mathbb{Z}_{2^2})^2 \times \mathbb{Z}_{463}$	$(\mathbb{Z}_{2^2})^2 \times (\mathbb{Z}_3)^2 \times \mathbb{Z}_{463}$	
			$\frac{T+\zeta^6}{T^2} + \frac{T}{T^2+T+\zeta^7} + \zeta^3$	$(\mathbb{Z}_3)^2 \times (\mathbb{Z}_5)^2 \times \mathbb{Z}_{151}$	$\mathbb{Z}_3 \times (\mathbb{Z}_5)^2 \times \mathbb{Z}_{151}$	

Table 1: Continued.

t	$p=q$	$D=\sum Q_i/(P_i^{r_i})+f$	Ideal class group	Divisor class group	∞
2	2	$\frac{T+1}{T^3}+\frac{T}{T^3+T+1}+T+1$		$\mathbb{Z}_2\times\mathbb{Z}_{2^2}\times\mathbb{Z}_5$	
		$\frac{T+1}{T^3}+\frac{T}{T^3+T+1}+T^5+T^2+T$		$\mathbb{Z}_2\times\mathbb{Z}_{2^2}\times\mathbb{Z}_{7^2}$	Totally
		$\frac{T^2}{(T+1)^3}+\frac{T+1}{T^2+T+1}+T^5+T^2+T+1$		$\mathbb{Z}_2\times\mathbb{Z}_{2^2}\times\mathbb{Z}_{17}$	ramified
	3	$\frac{1}{T^2+T+2}+\frac{1}{(T^2+1)^2}+T^2+2T+1$		$\mathbb{Z}_3\times\mathbb{Z}_3\times\mathbb{Z}_{3^2}\times\mathbb{Z}_{7^2}\times\mathbb{Z}_{157}$	
		$\frac{1}{T^2+T+2}+\frac{1}{(T^2+1)^2}+2T^2+T+2$		$\mathbb{Z}_2\times\mathbb{Z}_3\times\mathbb{Z}_3\times\mathbb{Z}_{3^2}\times\mathbb{Z}_{751}$	
		$\frac{1}{T^2+T+2}+\frac{1}{(T^2+1)^2}+T^2+T+2$		$\mathbb{Z}_{2^2}\times\mathbb{Z}_3\times\mathbb{Z}_3\times\mathbb{Z}_{3^2}\times\mathbb{Z}_{127}$	
	2	$\frac{T+1}{T^3}+\frac{T+1}{T^2+T+1}+\frac{T}{T^3+T+1}$	$\mathbb{Z}_2\times\mathbb{Z}_{2^2}$	$\mathbb{Z}_2\times\mathbb{Z}_{2^3}\times\mathbb{Z}_5$	
		$\frac{T+1}{T^3}+\frac{T^5+T^3+1}{(T^2+T+1)^5}+\frac{T}{T^3+T+1}$		$\mathbb{Z}_2\times\mathbb{Z}_{2^2}\times\mathbb{Z}_5\times\mathbb{Z}_{29}$	Splits
		$\frac{T^4}{(T^2+T+1)^3}+\frac{T^2+T+1}{(T^4+T+1)^3}+\frac{T^5+1}{(T^3+T^2+1)^3}$		$\mathbb{Z}_2\times\mathbb{Z}_{2^2}\times\mathbb{Z}_{17}\times\mathbb{Z}_{8839}$	completely

Table 2: Infinite families of Artin–Schreier extensions $K=k(\alpha_D)$ over k whose λ_1-rank of the ideal class groups is t, λ_2-rank is $t-1$, and λ_3-rank is $t-2$, where $\alpha_D^p-\alpha_D=D$.

t	$p=q$	$D=\sum Q_i/(P_i^{r_i})+f$	Ideal class group	Divisor class group	∞
	3	$\frac{T^3+T+1}{(T^2+T+2)^2}+\frac{T^4+T^2+1}{(T^3+2T^2+1)^2}+\frac{T^4+2T+2}{(T^3+2T+1)^2}$	$(\mathbb{Z}_2)^2\times(\mathbb{Z}_3)^2\times\mathbb{Z}_{3^2}$	$(\mathbb{Z}_2)^2\times(\mathbb{Z}_3)^2\times\mathbb{Z}_{3^2}$	
				$\times\mathbb{Z}_{13}\times\mathbb{Z}_{787}\times\mathbb{Z}_{1693}$	
		$\frac{T^3+T+1}{(T^2+T+2)^2}+\frac{T^4+T^3+T^2+1}{(T^3+2T^2+1)^2}+\frac{T^4+2T+2}{(T^3+2T+1)^2}$		$(\mathbb{Z}_2)^2\times\mathbb{Z}_3\times\mathbb{Z}_{3^2}\times\mathbb{Z}_7$	
				$\times\mathbb{Z}_{13}\times\mathbb{Z}_{103}\times\mathbb{Z}_{84211}$	
		$\frac{T^3+T+1}{(T^2+T+2)^2}+\frac{T^4+T^2+1}{(T^3+2T^2+1)^2}+\frac{T^4+2T+2}{(T^3+T^2+2)^2}$		$(\mathbb{Z}_{2^2})^2\times(\mathbb{Z}_3)^2\times(\mathbb{Z}_3)^2$	
				$\times\mathbb{Z}_{61}\times\mathbb{Z}_{327667}$	
	2	$\frac{T+1}{T^2+T+1}+\frac{T^3}{T^4+T^3+T^2+T+1}+1$	$\mathbb{Z}_2\times\mathbb{Z}_{2^2}\times\mathbb{Z}_{5^2}$	$(\mathbb{Z}_2)^2\times\mathbb{Z}_{5^2}$	
		$\frac{1}{T^2+T+1}+\frac{T^3}{T^4+T^3+T^2+T+1}+1$	$\mathbb{Z}_2\times\mathbb{Z}_{2^2}\times\mathbb{Z}_7$	$(\mathbb{Z}_2)^2\times\mathbb{Z}_7$	
		$\frac{T+1}{T^2+T+1}+\frac{T^3}{T^4+T+1}+1$	$\mathbb{Z}_2\times\mathbb{Z}_{2^2}\times\mathbb{Z}_3\times\mathbb{Z}_7$	$(\mathbb{Z}_2)^2\times\mathbb{Z}_3\times\mathbb{Z}_7$	
	3	$\frac{T+2}{T^3+2T+1}+\frac{T^2+1}{(T^3+2T^2+1)^2}+1$	$(\mathbb{Z}_3)^2\times(\mathbb{Z}_{3^2})^2\times\mathbb{Z}_{13}\times\mathbb{Z}_{379}$	$\mathbb{Z}_3\times(\mathbb{Z}_{3^2})^2\times\mathbb{Z}_{13}\times\mathbb{Z}_{379}$	Inert
		$\frac{2T^2+2T+2}{T^3+2T+1}+\frac{T^2+1}{(T^3+2T^2+1)^2}+1$	$(\mathbb{Z}_3)^3\times\mathbb{Z}_{3^2}\times\mathbb{Z}_{19}\times\mathbb{Z}_{433}$	$(\mathbb{Z}_3)^4\times\mathbb{Z}_{19}\times\mathbb{Z}_{433}$	
		$\frac{2T^2+2}{T^3+2T+1}+\frac{T^2+1}{(T^3+2T^2+1)^2}+1$	$(\mathbb{Z}_3)^2\times\mathbb{Z}_{3^2}\times\mathbb{Z}_7\times\mathbb{Z}_{1303}$	$(\mathbb{Z}_3)^3\times\mathbb{Z}_7\times\mathbb{Z}_{1303}$	

Table 2: Continued.

over k whose λ_1-rank of the ideal class groups is t, λ_2-rank is $t-1$, and λ_3-rank is $t-2$ (Theorem 5.1). In the tables, we denote $\mathbb{Z}/m\mathbb{Z}$ by $\mathbb{Z}_m$ for a positive integer m.

Acknowledgment The authors would like to thank the reviewer for his/her valuable comments for improving the clarity of this paper; in particular, we added Remark 5.5 based on the reviewer's comments. Some partial results of this paper (Section 4) were obtained in the Ph.D. thesis [21] of the first author under the supervision of Prof. Yoonjin Lee.

References

[1] B. Anglés and J. Jaulent, *Théorie des genres des corps globaux*. Manuscripta Math. **101**(2000), 513–532.
[2] S. Bae, S. Hu, and H. Jung, *The generalized Rédei-matrix for function fields*. Finite Fields Appl. **18**(2012), 760–780.
[3] S. Bae and J. K. Koo, *Genus theory for function fields*. J. Aust. Math. Soc. Ser. A **60**(1996), 301–310.
[4] V. Bautista-Ancona, J. Diaz-Vargas, and J. A. Lara Rodríguez, *Imaginary quadratic function fields with ideal class group of prime exponent*. J. Number Theory **173**(2017), 243–253.
[5] P. E. Conner and J. Hurrelbrink, *Class number parity*, World Scientific, Singapore, 1988.
[6] C. F. Gauss, *Disquisitiones arithmeticae*, Springer, New York, 1801.
[7] H. Hasse, *Theorie der relativ-zyklischen algebraischen Funktionenkörper, insbesondere bei endlichem Konstantenkörper*. J. Reine Angew. Math. **172**(1934), 37–54.
[8] S. Hu and Y. Li, *The genus fields of Artin–Schreier extensions*. Finite Fields Appl. **16**(2010), 255–264.
[9] A. Iadarola, *On the 8-rank of quadratic class groups*, Master's thesis, Universiteit Leiden, 2017.
[10] H. Ichimura, *Quadratic function fields whose class numbers are not divisible by three*. Acta Arith. **91**(1999), no. 2, 181–190.
[11] Y. Lee and J. Yoo, *Indivisibility of divisor class numbers of Kummer extensions over the rational function field*. J. Number Theory **192**(2018), 270–292.
[12] R. Lidl and H. Niederreiter, *Finite fields*, Cambridge University Press, Cambridge, 2003.
[13] G. Peng, *The ideal class group of function fields*. J. Sichuan Univ. **36**(1999), no. 4, 652–659.
[14] G. Peng, *The genus fields of Kummer function fields*. J. Number Theory **98**(2003), 221–227.
[15] L. Rédei and H. Reichardt, *Die anzahl der durch 4 teilbaren invarianten der Klassengruppe eines beliebigen quadratischen zahlkörpers*. J. Reine Angew. Math. **170**(1933), 69–74.
[16] M. Rosen, *Ambiguous divisor classes in function fields*. J. Number Theory **9**(1977), 160–174.
[17] M. Rosen, *Number theory in function fields*, Springer, New York, 2002.
[18] H. Stichtenoth, *Algebraic function fields and codes*, Springer, Berlin–Heidelberg, 2009.
[19] C. Wittmann, *l-class groups of cyclic function fields of degree l*. Finite Fields Appl. **13**(2007), 327–347.
[20] C. Wittmann, *l-parts of divisor class groups of cyclic function fields of degree l*. Int. J. Number Theory **3**(2007), no. 2, 171–190.
[21] J. Yoo, *Class groups of cyclic extensions over the rational function field*, Dissertation, Ewha Womans University, 2019.
[22] J. Yoo and Y. Lee, *Infinite families of cyclotomic function fields with any prescribed class group rank*. J. Pure Appl. Algebra **225**(2021), no. 9, Article no. 106658, 22 pp.
[23] Q. Yue, *The generalized Rédei-matrix*. Math. Z. **261**(2009), no. 1, 23–37.
[24] Z. Zhao, *3-class groups of cubic cyclic function fields*. Turk. J. Math. **42**(2018), no. 5, 2607–2620.
[25] Z. Zhao and W. Hu, *On l-class groups of global function fields*. Int. J. Number Theory **12**(2016), no. 2, 341–356.

Department of Mathematical Sciences, Ulsan National Institute of Science and Technology, 50, UNIST-Gil, Ulsan 44919, Republic of Korea
e-mail: jinjooyoo@unist.ac.kr

Department of Mathematics, Ewha Womans University, 52, Ewhayeodae-Gil, Seodaemun-Gu, Seoul 03760, Republic of Korea
e-mail: yoonjinl@ewha.ac.kr